#2

THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the Application of : **Katsuichi NAKAMURA, et al.**

Filed : **Concurrently herewith**

For : **NETWORK ACCESS CONTROL METHOD,.....**

Serial No. : **Concurrently herewith**

March 26, 2001

Assistant Commissioner of Patents
Washington, D.C. 20231

SUBMISSION OF PRIORITY DOCUMENT

S I R:

Attached herewith are Japanese patent application No. 2000-331345 of October 30, 2000 whose priority has been claimed in the present application.

Respectfully submitted

[ ]Samson Helfgott
Reg. No. 23,072
[x]Aaron B. Karas
Reg. No. 18,923

HELFGOTT & KARAS, P.C.
60th FLOOR
EMPIRE STATE BUILDING
NEW YORK, NY 10118
DOCKET NO.:FUJI 18.503
BHU:priority

Filed Via Express Mail
Rec. No.: EL522402486US
On: March 26, 2001
By: Brendy Lynn Belony
Any fee due as a result of this paper, not covered by an enclosed check may be charged on Deposit Acct. No. 08-1634.

日本国特許庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２０００年１０月３０日

出願番号
Application Number: 特願２０００－３３１３４５

出願人
Applicant (s): 富士通株式会社

CERTIFIED COPY OF PRIORITY DOCUMENT

２００１年 ２月２３日

特許庁長官
Commissioner,
Patent Office 及川耕造

出証番号 出証特２００１－３０１１２５８

【書類名】　特許願

【整理番号】　0051762

【提出日】　平成12年10月30日

【あて先】　特許庁長官　及川　耕造　殿

【国際特許分類】　H04L 12/40

【発明の名称】　ネットワークアクセス制御方法及びそれを用いたネットワークシステム及びそれを構成する装置

【請求項の数】　5

【発明者】

【住所又は居所】　福岡県福岡市早良区百道浜２丁目２番１号　富士通西日本コミュニケーション・システムズ株式会社内

【氏名】　中村　勝一

【発明者】

【住所又は居所】　福岡県福岡市早良区百道浜２丁目２番１号　富士通西日本コミュニケーション・システムズ株式会社内

【氏名】　山村　新也

【発明者】

【住所又は居所】　福岡県福岡市早良区百道浜２丁目２番１号　富士通西日本コミュニケーション・システムズ株式会社内

【氏名】　佐藤　義治

【特許出願人】

【識別番号】　000005223

【氏名又は名称】　富士通株式会社

【代理人】

【識別番号】　100070150

【住所又は居所】　東京都渋谷区恵比寿４丁目２０番３号　恵比寿ガーデンプレイスタワー３２階

【弁理士】

【氏名又は名称】　伊東　忠彦

【電話番号】　03-5424-2511

【手数料の表示】

【予納台帳番号】　002989

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9704678

【プルーフの要否】　要

【書類名】　　明細書

【発明の名称】　ネットワークアクセス制御方法及びそれを用いたネットワークシステム及びそれを構成する装置

【特許請求の範囲】

【請求項１】　パケットフィルタリング機能を有するネットワーク装置と、

前記ネットワーク装置を介してＩＰネットワークに接続され、ユーザにサービスを提供するサービスサーバと、

前記ネットワーク装置を介してＩＰネットワークに接続されサービスサーバが提供するサービスを利用するためのユーザ端末と、

前記ＩＰネットワークに接続されサービスサーバの受付としてユーザ端末からのアクセスを受け付ける受付サーバと、

前記ネットワーク装置を制御するアクセス制御サーバと、で構成されるネットワークシステムのネットワークアクセス制御方法において、

前記受付サーバは、ユーザ端末からのアクセス要求情報を受信して保持し、

前記アクセス制御サーバは、前記サービスサーバの処理能力及びサービスサーバへのトラヒック量に基づき最適に処理可能なアクセス要求分だけ前記アクセス登録手段に保持されたアクセス要求情報を抽出して前記サービスサーバへのアクセスを許容するトラヒック制御を行うことを特徴とするネットワークアクセス制御方法。

【請求項２】　パケットフィルタリング機能を有するネットワーク装置と、

前記ネットワーク装置を介してＩＰネットワークに接続され、ユーザにサービスを提供するサービスサーバと、

前記ネットワーク装置を介してＩＰネットワークに接続されサービスサーバが提供するサービスを利用するためのユーザ端末と、

前記ＩＰネットワークに接続されサービスサーバの受付としてユーザ端末からのアクセスを受け付けるアクセス受付手段を備えた受付サーバと、

前記ネットワーク装置を制御するトラヒック制御手段を備えたアクセス制御サーバと、で構成されるネットワークシステムにおいて、

前記受付サーバは、前記アクセス受付手段を介しユーザ端末からのアクセス要

求情報を受信して保持するアクセス登録手段を有し、

前記アクセス制御サーバは、前記サービスサーバの処理能力及びサービスサーバへのトラヒック量に基づき最適に処理可能なアクセス要求分だけ前記アクセス登録手段に保持されたアクセス要求情報を抽出して前記サービスサーバへのアクセスを許容するトラヒック制御を行うフィルタリング最適化手段を有することを特徴とするネットワークシステム。

【請求項３】　ユーザ端末からのアクセス要求情報を保持するアクセスリストと、

各ユーザのユーザクラスを含むユーザ情報を保持するユーザプロファイルと、

ユーザ端末からのアクセスを受け付けるアクセス受付手段と、

前記アクセス受付手段を介し受信したアクセス要求情報を前記アクセスリストに受付順に登録するアクセス登録手段と、

受信したアクセス要求情報からＩＰアドレスを抽出し、ＩＰアドレスによりユーザを特定して前記ユーザプロファイルからユーザクラスを抽出するユーザクラス抽出手段と、

前記アクセス受付手段を介し受信したアクセス要求情報を前記ユーザクラス抽出手段で抽出したユーザクラスに基づいて前記アクセスリストに登録するユーザクラス別アクセス登録手段を

有することを特徴とする受付サーバ。

【請求項４】　請求項３記載の受付サーバにおいて、

ユーザ端末からのアクセス要求を受け付けて前記アクセスリストへ登録する位置に応じた待ち合わせを行っているユーザ数から予測待ち合わせ時間を算出する予測待合時間算出手段と、

算出した予測待ち合わせ時間の情報をユーザに通知し予測待ち合わせ時間経過後、ユーザ端末にアクセス可能であることを通知するアクセス情報通知手段を

有することを特徴とする受付サーバ。

【請求項５】　請求項３記載の受付サーバにおいて、

ユーザ端末からのアクセス要求を受け付けた際に、待ち合わせが必要な場合、前記アクセス要求をアクセスリストに登録するか否かをユーザ端末に確認するア

クセス確認手段と、

前記アクセス確認手段の確認をユーザ端末に通知する待合せ確認通知手段を有することを特徴とする受付サーバ。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、ネットワークアクセス制御方法及びそれを用いたネットワークシステム及びそれを構成する装置に関し、特に、ＩＰネットワークのネットワークアクセス制御方法及びそれを用いたネットワークシステム及びそれを構成する装置に関する。

【０００２】

【従来の技術】

従来のネットワークアクセス制御方法として、プロキシー・サーバによるアクセス制限方法がある。プロキシー・サーバとは、マルチメディア・データベース、ＷＷＷ（Ｗｏｒｌｄ　Ｗｉｄｅ　Ｗｅｂ）など、インターネットの様々なサービスへのアクセスを中継するためのソフトウエア、またはサーバー・マシンである。

【０００３】

プロキシー・サーバーは、社内ネットワークとインターネット間のトラフィックを軽減したい時などキャッシュ機能として使用する。例えば、社内のユーザーがあるＷＷＷのページのアクセスすると、その内容をプロキシーサーバーは一定期間記憶しておく。次に別のユーザーが同じページにアクセスした場合は、インターネットにアクセスする必要はなく、プロキシーサーバーが持つ情報をユーザーに返送する。このようにしてインターネット・アクセスの頻度を減らせる。

【０００４】

また、サーバアプリケーションで、接続コネクション数を予め設定するアクセス制限方法がある。例えば特開平５－３１６１１５公報に記載のものは、複数の端末を接続するコンピュータネットワークを複数相互接続し、日付・曜日・時間あるいはグループ番号等によるアクセス制御をすることで、専用回線の負荷分散

を効率よく正確に行えることを目的とし、予め設定した情報テーブル（日付・曜日・時間、グループ番号からなる）を参照し、ネットワークのアクセス制御を行う。

【０００５】

また、特開平６－１５２６１５公報に記載のように、複数伝送路の効率的な均等負荷制御を行うことを目的とし、伝送路の負荷計測機能と伝送路切替え制御機能を具備して、伝送路対応の負荷（トラヒック量）を計測して負荷の低い経路を選択することを特徴とするネットワークアクセス制御方法がある。

【０００６】

更に、トラヒックが集中するサーバに対する負荷分散を目的とし、複数のミラーサーバを設け、サーバとミラーサーバの負荷状況を計測しミラーサーバから最も負荷の低いサーバにアクセスさせるという負荷バランスシステムも提案されている。

【０００７】

【発明が解決しようとする課題】

プロキシー・サーバを使用した方法では、コンテンツ・オブジェクトが一度キャッシュに蓄えられた後、情報発信元のオブジェクトが更新された場合、２回目以降はオブジェクトの実体にアクセスしないのでオブジェクトが更新されず、何回リクエストしても新しい情報が入手できないことになる。さらに、サーチエンジンの検索結果でアクセスする度に内容が変化する（カウンタなど）動的なオブジェクトは再利用できない。また、キャッシュ機能にもメモリ容量やディスク容量の制限があるため、有効と思われるオブジェクトでも状況によって消去しなければならないという問題がある。

【０００８】

接続コネクション数を予め設定する方法は、トラヒック集中時に利用者は何度もアクセスしないとならないので、無意味なトラヒックがネットワーク上を流れる事になる。更に、予め設定した情報（日付・曜日・時間）によって、またはトラヒック量を計測することによって負荷の低い経路を選択した場合でも、接続先のサーバがそれに耐えられる処理能力を持たないと最適な経路選択は効果を十分

生かせないという問題がある。

【０００９】

また、サーバとミラーサーバの負荷状況を計測し負荷の低いサーバにアクセスさせる方法は、利用者からのアクセスを割り振っただけなので、サーバやミラーサーバ毎に発生する高負荷の場合のアクセス制御は行われない。トラヒックが集中するサーバに対しては、ネットワーク側でもアクセス規制を行わないとミラーサーバを無意味に増やすだけになるという問題がある。

【００１０】

本発明は、上記の点に鑑みなされたものであり、動的オブジェクトを再利用でき、トラヒックの軽減を図ることができ、ユーザに与える負担を軽減でき、アクセス要求したユーザは自分のアクセス順番になれば速い応答速度で快適にサービスを受けることが可能となるネットワークアクセス制御方法及びそれを用いたネットワークシステム及びそれを構成する装置を提供することを目的とする。

【００１１】

【課題を解決するための手段】

請求項１に記載の発明は、パケットフィルタリング機能を有するネットワーク装置と、

前記ネットワーク装置を介してＩＰネットワークに接続され、ユーザにサービスを提供するサービスサーバと、

前記ネットワーク装置を介してＩＰネットワークに接続されサービスサーバが提供するサービスを利用するためのユーザ端末と、

前記ＩＰネットワークに接続されサービスサーバの受付としてユーザ端末からのアクセスを受け付ける受付サーバと、

前記ネットワーク装置を制御するアクセス制御サーバと、で構成されるネットワークシステムのネットワークアクセス制御方法において、

前記受付サーバは、ユーザ端末からのアクセス要求情報を受信して保持し、

前記アクセス制御サーバは、前記サービスサーバの処理能力及びサービスサーバへのトラヒック量に基づき最適に処理可能なアクセス要求分だけ前記アクセス登録手段に保持されたアクセス要求情報を抽出して前記サービスサーバへのアク

セスを許容するトラヒック制御を行うため、

ユーザがサービスサーバにアクセスする場合に、サービスサーバの処理能力及びサービスサーバへのトラヒック量に見合う分だけのユーザからのアクセスが許容され、動的オブジェクトを再利用できると共にトラヒックの軽減を図ることができる。

【００１２】

請求項２に記載の発明は、パケットフィルタリング機能を有するネットワーク装置と、

前記ネットワーク装置を介してＩＰネットワークに接続され、ユーザにサービスを提供するサービスサーバと、

前記ネットワーク装置を介してＩＰネットワークに接続されサービスサーバが提供するサービスを利用するためのユーザ端末と、

前記ＩＰネットワークに接続されサービスサーバの受付としてユーザ端末からのアクセスを受け付けるアクセス受付手段を備えた受付サーバと、

前記ネットワーク装置を制御するトラヒック制御手段を備えたアクセス制御サーバと、で構成されるネットワークシステムにおいて、

前記受付サーバは、前記アクセス受付手段を介しユーザ端末からのアクセス要求情報を受信して保持するアクセス登録手段を有し、

前記アクセス制御サーバは、前記サービスサーバの処理能力及びサービスサーバへのトラヒック量に基づき最適に処理可能なアクセス要求分だけ前記アクセス登録手段に保持されたアクセス要求情報を抽出して前記サービスサーバへのアクセスを許容するトラヒック制御を行うフィルタリング最適化手段を有するため、

ユーザがサービスサーバにアクセスする場合に、サービスサーバの処理能力及びサービスサーバへのトラヒック量に見合う分だけのユーザからのアクセスが許容され、動的オブジェクトを再利用できると共にトラヒックの軽減を図ることができる。

【００１３】

請求項３に記載の発明は、ユーザ端末からのアクセス要求情報を保持するアクセスリストと、

各ユーザのユーザクラスを含むユーザ情報を保持するユーザプロファイルと、

ユーザ端末からのアクセスを受け付けるアクセス受付手段と、

前記アクセス受付手段を介し受信したアクセス要求情報を前記アクセスリストに受付順に登録するアクセス登録手段と、

受信したアクセス要求情報からＩＰアドレスを抽出し、ＩＰアドレスによりユーザを特定して前記ユーザプロファイルからユーザクラスを抽出するユーザクラス抽出手段と、

前記アクセス受付手段を介し受信したアクセス要求情報を前記ユーザクラス抽出手段で抽出したユーザクラスに基づいて前記アクセスリストに登録するユーザクラス別アクセス登録手段を有するため、

ユーザクラス別にユーザからのアクセス要求情報を登録することができる。

【００１４】

請求項４に記載の発明は、請求項３記載の受付サーバにおいて、

ユーザ端末からのアクセス要求を受け付けて前記アクセスリストへ登録する位置に応じた待ち合わせを行っているユーザ数から予測待ち合わせ時間を算出する予測待合時間算出手段と、

算出した予測待ち合わせ時間の情報をユーザに通知し予測待ち合わせ時間経過後、ユーザ端末にアクセス可能であることを通知するアクセス情報通知手段を有するため、

ユーザにサービスへのアクセス可能となるまでの時間を通知してユーザからのアクセス要求の待合せを可能とし、ユーザに与える負担を軽減できる。

【００１５】

請求項５に記載の発明は、請求項３記載の受付サーバにおいて、

ユーザ端末からのアクセス要求を受け付けた際に、待ち合わせが必要な場合、前記アクセス要求をアクセスリストに登録するか否かをユーザ端末に確認するアクセス確認手段と、

前記アクセス確認手段の確認をユーザ端末に通知する待合せ確認通知手段を有するため、

ユーザに待合せを行うことを確認することができる。

【００１６】

付記６に記載の発明は、サービスサーバの処理能力に関する情報及びサービスサーバの処理能力に基づき算出された最大アクセス許容数を保持するアクセス情報データベースと、

ネットワーク装置を制御するトラヒック制御手段と、

前記サービスサーバの処理能力に関する情報に基づき最大アクセス許容数を算出する静的アクセス許容数算出手段と、

受付サーバでユーザ端末からのアクセス要求情報を保持するアクセスリストの先頭から最大アクセス許容数分のアクセス要求情報を読み出し、アクセス要求を行ったユーザ端末をサービスサーバにアクセス可能とするパケットフィルタリング設定情報を生成し前記トラヒック制御手段を介して前記ネットワーク装置に設定するフィルタリング最適化手段を有するため、

サービスサーバの処理能力に見合うユーザからのアクセスを受け付ける制御を行うことができる。

【００１７】

付記７に記載の発明は、付記６記載のアクセス制御サーバにおいて、

前記サービスサーバの負荷状態及びサービスサーバを収容するネットワーク装置のトラフィック状態を監視する負荷・トラヒック監視装置と、

周期的に負荷・トラヒック監視装置と通信して前記負荷状態及びトラヒック状態の情報を抽出して前記アクセス情報データベースの最大アクセス許容数を算出すると共に、算出した最大アクセス許容数を前記アクセス情報データベースに登録する動的アクセス許容数算出手段を有するため、

サービスサーバの負荷状況やトラヒック状況に応じてサービスサーバが最適に動作可能なアクセス分のユーザにアクセスを許可することが可能となる。

【００１８】

付記８に記載の発明は、付記６記載のアクセス制御サーバにおいて、

ユーザ端末からのアクセス要求情報を前記アクセスリストから読み出す際に読み出す指針となる制御情報を保持する制御情報データベースと、

前記フィルタリング最適化手段が前記アクセスリストから最大アクセス許容数

分のアクセス要求情報を読み出す際に前記アクセスリストがユーザクラス別に登録されている場合、前記制御情報データベースから抽出された制御情報に基づき前記アクセスリストの各ユーザクラスからアクセス要求情報を読み出すユーザクラス別アクセス要求読出手段を有するため、

ユーザクラスに応じて読み出すアクセス要求情報数を可変することができる。

【００１９】

付記９に記載の発明は、付記６記載のアクセス制御サーバにおいて、

パケットフィルタリング設定情報を生成する際にアクセス要求情報に有効タイマを設定する有効タイマ設定手段と、

前記有効タイマの満了時にネットワーク装置に設定したパケットフィルタリング制御を解除するフィルタリング解除手段を有するため、

有効タイマを用いて各アクセスの時間管理を行い、アクセス許可を解除することができる。

【００２０】

付記１０に記載の発明は、ネットワーク装置を介してＩＰネットワークに接続され、ユーザにサービスを提供するサービスサーバにおいて、

ユーザ端末とのセッションを終了したこと判定するセッション終了判定手段と、

前記ユーザ端末とのセッションを終了したことをアクセス制御サーバに通知するセッション終了通知手段を有するため、

セッションが終了したアクセスのアクセス許可を解除することができる。

【００２１】

付記１１に記載の発明は、請求項３記載の受付サーバにおいて、

前記ユーザクラス抽出手段で抽出したユーザクラスに基づき前記アクセス受付手段を介し受信したアクセス要求が不許可のユーザからか否かを判定し、不許可ユーザであればアクセス制御サーバにその旨を通知するユーザ認証手段を有し、また、付記１２に記載の発明は、付記６記載のアクセス制御サーバにおいて、

付記１１記載の受付サーバのユーザ認証手段からの通知に基づき前記サービスサーバにアクセス不許可とするパケットフィルタリング設定情報を生成して前記

ネットワーク装置に設定するアクセス不許可フィルタリング設定手段を有するため、

ユーザがアクセス権限を持っている場合にのみサービスサーバのアクセスを許可することができる。

【発明の実施の形態】

図１は、本発明方法の一実施例の全体構成図を示す。同図中、コアネットワーク（ＩＰネットワーク）１０にはルータ等のネットワーク装置２０，３０，４０が設けられている。ネットワーク装置２０，３０はパケットフィルタリング機能を有しており、ネットワーク装置２０にはユーザ端末５０が接続され、ネットワーク装置３０にはユーザにサービスを提供するサービスサーバ３００が接続されている。

【００２２】

また、ネットワーク装置４０には、サービスサーバ３００の受付としてユーザからのアクセスを受け付ける受付サーバ１００と、ネットワーク装置４０を制御すると共にサービスサーバ３００の負荷状態やサービスサーバ３００を収容するネットワーク装置３０のトラフィック状態を監視するアクセス制御サーバ２００とが接続されている。

【００２３】

受付サーバ１００において、ユーザプロファイル１１１は、各ユーザのユーザクラス等のユーザ情報を保持する。アクセスリスト１０９は、ユーザからのアクセス要求情報を保持する。アクセス受付手段１１０は、ユーザからのアクセスを受け付ける。アクセス登録手段１０３は、アクセス受付手段１１０を介しユーザからのアクセス要求情報を受信し、このアクセス要求情報をアクセスリスト１０９に受付順に登録する。

【００２４】

ユーザクラス抽出手段１０２は、アクセス受付手段１０３を介しユーザからのアクセス要求情報を受信し、このアクセス要求情報からＩＰアドレスを抽出し、ＩＰアドレスによりユーザを特定し、ユーザプロファイルからユーザクラス抽出する。ユーザクラス別アクセス登録手段１０８は、ユーザクラス抽出手段１０２

を介し取得したユーザクラスに基づいて、アクセス要求情報をアクセスリストに登録する。予測待合時間算出手段１０６は、ユーザからのアクセス要求を受け付けた際に、本アクセス要求をアクセスリスト１０９に登録する位置から、既存のＡＩ機能及び統計手法等を用いて、予測待ち合わせ時間を算出する。アクセス情報通知手段１０７は、算出した予測待ち合わせ時間の情報をユーザに通知し、予測待ち合わせ時間経過後、ユーザにアクセス可能であることを通知する。

【００２５】

アクセス確認手段１０４は、ユーザからのアクセス要求を受け付けた際に、本アクセス要求をアクセスリスト１０９に登録するか否かをユーザに確認する。待合せ確認通知手段１０５は、アクセス要求をアクセスリスト１０９に登録するか否かをユーザに確認通知する。ユーザ認証手段１０１は、ユーザクラス抽出手段１０２を介し取得したユーザクラスに基づいてアクセス要求が不許可のユーザからか否かを判定し、不許可ユーザであればアクセス制御サーバ２００にその旨を通知する。

【００２６】

アクセス制御サーバ２００において、アクセス情報ＤＢ（データベース）２０９は、サービスサーバ３００の処理能力に関する情報、及びサービスサーバの処理能力に基づき算出された最大アクセス許容数を保持する。制御情報ＤＢ（データベース）２１１は、ユーザからのアクセス要求情報をアクセスリスト１０９から読み出す際に、読み出す指針となる制御情報を保持する。トラヒック制御手段２１０は、ネットワーク装置４０を制御する。負荷・トラヒック監視装置２１２は、サービスサーバ３００の負荷状態やサービスサーバ３００を収容するネットワーク装置３０のトラフィック状態を監視する。

【００２７】

静的アクセス許容数算出手段２０６は、サービスサーバ３００の処理能力に関する情報に基づき最大アクセス許容数を算出する。フィルタリング最適化手段２０４は、アクセスリスト１０９の先頭から最大アクセス許容数分のアクセス要求情報を読み出し、アクセス要求を行ったユーザ端末をサービスサーバ３００にアクセス可能とするパケットフィルタリング設定情報を生成し、このパケットフィ

ルタリング設定情報をトラヒック制御手段２１０を介して、ネットワーク装置２０，３０に設定する。動的アクセス許容数算出手段２０７は、周期的に負荷・トラヒック監視装置２１２と通信して負荷状態及びトラヒック状態の情報を抽出し、アクセス情報ＤＢ２０９の最大アクセス許容数を算出すると共に、算出した最大アクセス許容数をアクセス情報ＤＢ２０９に登録する。

【００２８】

ユーザクラス別アクセス要求読出手段２０５は、フィルタリング最適化手段２０４が、アクセスリスト１０９から最大アクセス許容数分のアクセス要求情報を読み出す際に、アクセスリスト１０９がユーザクラス別に登録されている場合、制御情報ＤＢ２１１から読み出す指針となる制御情報を抽出し、この制御情報に基づき、各ユーザクラスからアクセス要求情報を読み出す。有効タイマ設定手段２０３は、パケットフィルタリング設定情報を生成する際に、アクセス要求情報に有効タイマを設定する。

【００２９】

フィルタリング解除手段２０２は、有効タイマ満了時にネットワーク装置に設定したパケットフィルタリング制御を解除する。セッション完了フィルタリング解除手段２０８は、サービスサーバ３００がユーザにサービスを提供する際に、セッション途中でユーザからのアクセスが不許可になることを防止するため、サービスサーバからセッションを終了したことを受信した際に、ネットワーク装置に設定したパケットフィルタリング制御を解除する。アクセス不許可フィルタリング設定手段２０１は、サービスサーバ３００にアクセス不許可とするパケットフィルタリング設定情報を生成し、その情報をネットワーク装置２０，３０に設定する。

【００３０】

サービスサーバ３００において、セッション終了判定手段３０２は、ユーザとのセッションを終了したことを判定する。セッション終了通知手段３０１は、サービスサーバがユーザにサービスを提供する際に、セッション途中でユーザからのアクセスが不許可になるとを防止するため、ユーザとのセッションを終了したことをアクセス制御サーバ２００に通知する。

【００３１】

ここで、本発明方法のパケットフィルタリング機能について、図１の一部を抜粋した図２を用いて説明する。なお、図２～図９において、矢印に付した括弧付きの符号は文中の括弧付きの符号を対応させている。

【００３２】

図２において、ユーザは、ユーザ端末５０よりサービスサーバ３００へのアクセス要求を受付サーバ１００に送信する（１）。受付サーバ１００のアクセス受付手段１１０は、アクセス要求情報を受信しアクセス登録手段１０３にその情報を渡す（２）。アクセス登録手段１０３は、受付順にアクセス要求情報をアクセスリスト１０９に登録する（３）。そして、アクセス制御サーバ２００のフィルタリング最適化手段２０４にフィルタリング要求を行う（４）。

【００３３】

そして、アクセス制御サーバ２００のフィルタリング最適化手段２０４は、受付サーバ１００のアクセス登録手段１０３からフィルタリング要求を受け、アクセス先のサービスサーバ３００の処理能力に基づき静的アクセス許容数算出手段２０６で算出された（０）最大アクセス許容数をアクセス情報ＤＢ２１１より抽出し（５）、アクセスリスト１０９から最大アクセス許容数分のアクセス情報を読み出す（６）。次に、アクセス要求を行ったユーザ端末５０のサービスサーバ３００に対するアクセスを許可するパケットフィルタリング許可情報を生成し、パケットフィルタリング許可要求をトラヒック制御手段に行う（７）。トラヒック制御手段２１０は、それら情報に基づいてネットワーク装置２０，３０を制御する（８）。

【００３４】

また、上記の説明では、アクセス登録手段１０３は受付順にアクセス要求情報をアクセスリスト１０９に登録したが、別手段として、アクセス登録手段１０３は、ユーザクラス別アクセス登録を行う必要があれば、ユーザクラス別アクセス登録手段１０８にユーザクラス別アクセス登録要求を行う（３－１）。ユーザクラス別アクセス登録手段１０８は、ユーザクラスの問合わせをユーザクラス抽出手段１０２に行う（３－２）。

【００３５】

ユーザクラス抽出手段１０２は、前記アクセス要求情報からＩＰアドレスを抽出し、ＩＰアドレスによりユーザを特定し、ユーザプロファイル１１１からユーザクラスを抽出し（３－３）、抽出したユーザクラスをユーザクラス別アクセス登録手段１０８に返す（３－４）。そして、ユーザクラス別アクセス登録手段１０８は、取得したユーザクラスに基づいて、アクセス要求情報をアクセスリスト１０９に登録する（３－５）。

【００３６】

次に、本発明方法の予測待合時間通知機能について、図１の一部を抜粋した図３を用いて説明する。

【００３７】

図３において、ユーザは、ユーザ端末５０よりサービスサーバ３００へのアクセス要求を受付サーバに送信する（１）。アクセス受付手段１１０は、受信したアクセス要求をアクセスリストに登録するようアクセス登録手段１０３に要求する（２）。アクセス登録手段１０３は、空きのアクセスリスト１０９がない過負荷の場合、予測待合時間算出手段１０８へ予約待合時間算出要求をする（３）。予測待合時間算出手段１０８は、アクセスリスト１０９を参照し、本アクセス要求情報の登録位置に応じた待ち合わせを行っているユーザ数から予測待合時間を算出し、アクセス情報通知手段へユーザ通知要求をする（４）。アクセス情報通知手段１０７は、アクセス要求対象ユーザのユーザ端末５０に対して、予測待合時間を通知する（５）。

【００３８】

次に、本発明方法の予測待合時間通知機能について、図１の一部を抜粋した図４を用いて説明する。

【００３９】

図４において、ユーザはユーザ端末５０よりサービスサーバ３００へのアクセス要求を受付サーバ１００に送信する（１）。アクセス受付手段１１０は、受信したアクセス要求をアクセスリスト１０９に登録するようアクセス登録手段１０３に要求する（２）。アクセス登録手段１０３は、アクセス要求情報をアクセス

リスト１０９に登録するか否かを確認する場合、つまり、待ち合わせが必要である場合は、アクセス確認手段１０４にアクセスリスト１０９の登録確認を行う（３）。アクセス確認手段１０４は、アクセス要求情報からユーザ端末５０のＩＰアドレスを抽出し、抽出したＩＰアドレスにアクセスリスト登録確認通知を行うよう待合せ確認通知手段１０５に要求する（４）。待合せ確認通知手段１０５はユーザに確認メッセージを送信する（５）。

【００４０】

そして、ユーザは確認メッセージの応答をアクセス受付手段１１０に再度送信する（６）。アクセス受付手段１１０は、ユーザからの応答をアクセス登録手段１０３に送信し（７）、アクセス登録手段１０３は、ユーザからの応答が登録ならば、アクセスリスト１０９にアクセス要求情報を登録する（８）。

【００４１】

次に、本発明方法の動的アクセス許容数算出機能について、図１の一部を抜粋した図５を用いて説明する。

【００４２】

図５において、動的アクセス許容数算出手段２０７は、周期的に負荷・トラヒック監視装置２１２からサービスサーバ３００の負荷状態、及びサービスサーバ３００を収容するネットワーク装置のトラフィック状態の情報を抽出し、最大アクセス許容数を算出する（１）。そして、その最大アクセス許容数をアクセス情報ＤＢに設定する（２）。

【００４３】

次に、本発明方法のユーザクラス別アクセス要求読出機能について、図１の一部を抜粋した図６を用いて説明する。

【００４４】

図６において、ユーザクラス別にアクセスリスト１０９にアクセス要求情報を登録する場合は、アクセス登録手段１０３は、ユーザクラス別にアクセス要求情報を登録する要求をユーザクラス別アクセス登録手段１０８に行う（１）。ユーザクラス別アクセス登録手段１０８は、ユーザクラス別にアクセスリスト１０９にアクセス要求情報の登録をする（２）。そして、アクセス登録手段１０３は、

フィルタリング最適化手段２０４にフィルタリング要求を行う（３）。

【００４５】

フィルタリング要求を受けたフィルタリング最適化手段２０４は、ユーザクラス別にどのような割合でアクセス要求情報を読み出すかを、ユーザクラス別アクセス要求読出手段２０５に問い合わせる（４）。ユーザクラス別アクセス要求読出手段はアクセス情報ＤＢから最大アクセス許容数を抽出し（５）、制御情報ＤＢからユーザクラス別にどのような割合でアクセス要求情報を読み出すかという制御情報を抽出し（６）、それらの情報に基づいて、ユーザクラス別にアクセス要求情報をアクセスリスト１０９から抽出し（７－１）、フィルタリング最適化手段に送信する（７－２）。

【００４６】

次に、本発明方法の有効タイマ機能について、図１の一部を抜粋した図７を用いて説明する。

【００４７】

図７において、受付サーバ１００のアクセス登録手段１０３からフィルタリング要求をフィルタリング最適化手段２０４が受信すると（１－１）、フィルタリング最適化手段２０４は、ネットワーク装置２０，３０にパケットフィルタリング設定後、有効タイマ設定手段２０３に有効タイマ設定要求を行う（１－２）。有効タイマ設定手段２０３は、アクセスリスト１０９のアクセス要求情報に有効タイマ値を設定する（１－３）。

【００４８】

フィルタリング解除手段２０２は、周期的にアクセスリスト１０９の有効タイマの満了チェックを行う（２－１）。有効タイマ満了アクセス要求情報があれば、アクセスリスト１０９からそのアクセス要求情報を削除し、該当アクセス要求を行ったユーザ端末をサービスサーバ３００に対しアクセス許可からアクセス不許可とするパケットフィルタリング解除情報を生成し、トラヒック制御手段２１０に対してフィルタリング解除要求をする（２－２）。

【００４９】

次に、本発明方法のセッション終了機能について、図１の一部を抜粋した図８

を用いて説明する。

【００５０】

図８において、サービスサーバ３００は、ユーザとのセッションが終了した際に、セッション終了判定手段３０２からのセッション終了通知をセッション終了通知手段３０１に通知する（１）。セッション終了通知手段３０１は、その旨をアクセス制御サーバ２００のセッション完了フィルタリング解除手段２０８に送信する（２）。セッション完了フィルタリング解除手段２０８は、解除要求のあったコネクションに対して、ユーザ端末５０からサービスサーバ３００へのアクセスを許可から不許可とするパケットフィルタリング解除情報を生成し、トラヒック制御手段２１０に対してフィルタリング解除要求をする（３）。そして、トラヒック制御手段２１０は、パケットフィルタリング解除情報に基づいてネットワーク装置２０，３０を制御する（４）。

【００５１】

次に、本発明方法のアクセス不許可機能について、図１の一部を抜粋した図９を用いて説明する。

【００５２】

図９において、ユーザは、ユーザ端末５０よりサービスサーバ３００へのアクセス要求を受付サーバ１００のアクセス受付手段１１０に送信する（１）。アクセス受付手段１１０は、アクセス要求情報をユーザ認証手段１０１に送信する（２）。ユーザ認証手段１０１は、ユーザクラス抽出手段１０２を介して、ユーザプロファイル１１１よりアクセス要求を行ったユーザのユーザクラス（ユーザ情報）を抽出する（３）。その際に、対象ユーザがない場合や、ユーザクラスがアクセス不許可の場合は、アクセス不許可フィルタリング設定手段２０１に不許可のフィルタリング要求を行う（４－１）。

【００５３】

アクセス不許可フィルタリング設定手段は、アクセス不許可のフィルタリング要求を受け、アクセス要求を行ったユーザ端末をサービスサーバ３００にアクセス不許可とするパケットフィルタリング不許可情報を生成し、トラヒック制御手段２１０に対してフィルタリング不許可要求をする（４－２）。そして、トラヒ

ック制御手段２１０は、パケットフィルタリング不許可情報に基づいてネットワーク装置２０，３０を制御する（５）。

【００５４】

以下、本発明を用いた具体的なサービスの実施例を示し、処理の詳細を説明する。

【００５５】

Ａ．インターネットサービスプロバイダによる受付代行サービス

図１０は、インターネットサービスプロバイダが受付代行サービスを行う実施例のシステム構成図を示す。図１０に示すサイト（３１０）は、例えば人気商品のオンライン販売を予定しているサイトであり、アクセストラフィックの過度の集中が予想されている。このサイトはトラフィックの集中に備えて、サービスサーバ３００を構成する数台のサーバ群３１０及び負荷分散装置３２０を準備しているが、販売開始直後のトラフィック集中に対してサーバの輻輳を懸念している。

【００５６】

このサイトが加入しているサービスプロバイダはこのような、トラフィック集中が予想されるサイトに対して受付代行サービスを提供している。このサービスプロバイダは、受付サーバ１００を構成する十分な台数の負荷分散サーバ群１２０及び負荷分散装置１３０と、アクセス制御サーバ２００と、大容量の回線２２０からなる受付代行センタを構築している。

【００５７】

ユーザＡ，Ｂのユーザ端末５１，５２は、ネットワーク装置２０としてのダイアルアップルータ２１，２２を介してコアネットワーク１０に接続され、受付代行センタの負荷分散装置１３０はネットワーク装置４０としてのルータ４１に接続され、サイトの負荷分散装置３２０はネットワーク装置３０としてのルータ３１に接続されている。

【００５８】

まず、この実施例で記述されるデータ・テーブル、及びメッセージ・テーブルについての説明をする。

【００５９】

図１１は、ユーザプロファイル１１１のデータ構造を示す。ユーザプロファイル１１１は、ユーザ端末５１のＩＰアドレスである送信元ＩＰアドレス（１００．１００．２００．１０）、サービスサーバ３００のＩＰアドレスである送信先ＩＰアドレス（１００．１００．４００．１００）、サービスサーバ３００のサービス提供通信ポート番号である送信先ポート番号（WWWを使ったサービスの場合は８０であり、ｈｔｔｐを示す）、ユーザのサービス使用レベルの指標となるユーザクラス、例えば、高優先、中優先、低優先、不許可等のユーザクラスをデータとして設定される。このユーザプロファイルは送信元ＩＰアドレス及び送信先ＩＰアドレス毎に設定される。

【００６０】

図１２は、アクセス情報ＤＢ２０９のデータ構造を示す。アクセス情報ＤＢ２０９は、例えばサービスサーバ３００のＩＰアドレス（１００．１００．４００．１００）、このサイトのサービスサーバ３００が接続しているルータ（ネットワーク装置）５１のＩＰアドレス（１００．１００．４００．１）、パケットフィルタリングを設定する際のインタフェースを示すパケットフィルタリング機能種別（例えばＳＮＭＰ）、サイトのサーバの処理能力を示す処理能力データ、ポート単位の情報を示すポート情報からなる。

【００６１】

処理能力データはサービスサーバ３００の処理能力を示すデータ・テーブル（例えばＣＰＵ種別、搭載メモリサイズ等）であり、各データはパーセント表示される。例えば高速ＣＰＵの場合は１５０として初期アクセス許容数を１．５倍して最大アクセス許容数に設定することを示し、低速ＣＰＵの場合は５０として初期アクセス許容数を１／２倍して最大アクセス許容数に設定することを示す。

【００６２】

ポート情報は、更にポート番号、初期アクセス許容数、最大アクセス許容数、有効タイマ値からなる。例えば、契約時にサイトに提示された情報が、最大アクセス数＝１００、平均アクセス時間＝５分であった場合、ポート番号に８０（ｈｔｔｐを示す）、最大アクセス許容数に１００、有効タイマ値に７分（５分を補

正した値）を設定する。有効タイマ値は、サービスサーバ３００の管理者がサービスをユーザに提供する上で必要と思われるサーバとユーザとのコネクション時間である。有効タイマ値は事前に受付代行センタにサービスサーバ３００の管理者が申請するものである。

【００６３】

また、アクセス情報ＤＢ２０９はネットワーク装置をアクセス制御するために、ユーザ用のデータとしても使用されるが、その場合は、ＩＰアドレス、ネットワーク装置ＩＰアドレス、パケットフィルタリング機能種別のみのデータが設定されており、その他のデータは設定されていない。

【００６４】

図１３は、アクセスリスト１０９のデータ構造を示す。アクセスリスト１０９は、サービスサーバ３００のＩＰアドレスである送信先ＩＰアドレス（１００．１００．４００．１００）、対象アプリケーションのポート番号である送信先ポート番号（例えば８０）、優先制御の有無を示す優先制御フラグ、ユーザからサービスサーバ３００へのアクセス要求をキューイングするアクセスリストから構成される。アクセスリストは、優先制御フラグが優先制御なしの場合に使用されるアクセスリストと、優先制御ありの場合に使用される優先度（高優先・中優先・低優先等）で分けられた高優先アクセスリスト、中優先アクセスリスト、低優先アクセスリストがある。

【００６５】

各アクセスリストは現在ユーザが対象とするサーバに接続可能かどうかを示す過負荷フラグ、接続中ユーザのキュー（バッファ・エリア）である接続中アクセスリストのポインタ、及び接続中アクセスリストにキューイングされている接続中のユーザ数である接続中ユーザ数、接続待ちユーザのキューである接続待ちリストのポインタ、及び接続待ちアクセスリストにキューイングされている接続待ちのユーザ数である接続待ちユーザ数からなる。

【００６６】

優先制御フラグは、サービスサーバ３００の管理者がユーザクラス別の優先制御を希望する場合に、事前にサービスサーバ３００の管理者が受付代行センタに

申請することで、優先制御フラグが優先制御ありで設定される。過負荷フラグは、現在ユーザがアクセスを要求するサーバに接続の空きがあるか否かを判定するためのフラグである。

【００６７】

また、空きバッファリストの先頭を示す空きバッファポインタ、有効タイマ切れの時刻でキューイングされている有効タイマ順ポインタがある。

【００６８】

図１４は、制御情報ＤＢ２１１を示す。制御情報ＤＢ２１１は、受付代理センタが提供する優先制御を行う場合のユーザクラス数であるユーザクラス数（例えば、高優先・中優先・低優先の場合は、３が設定される）、優先制御を希望するサービスサーバ３００毎に設定される読出制御データが設定されている。読出制御データはサービスサーバ３００のＩＰアドレスと、対象アプリケーションのポート番号であるポート番号毎にアクセスリスト１０９からユーザクラス別に読み出す比率である読出比率が設定されている。

【００６９】

次に、図１０に示すインターネットサービスプロバイダが受付代行サービスを実施する場合について説明する。

（１）受付代行サービスの契約

図１０に示すサイトｓｅｒｖｉｃｅ．ｃｏｍは、サービスプロバイダと受付代行サービスを契約する。契約時にｓｅｒｖｉｃｅ．ｃｏｍは、自サイトへのｈｔｔｐアドレス、ＩＰアドレス、自サイトのサーバ処理能力（最大処理数、一人あたりの平均アクセス時間等）をサービスプロバイダに提示する。

【００７０】

サービスプロバイダは、サイトから提示された情報を図１２に示すアクセス情報ＤＢ２０９に登録し、例えば、ｈｔｔｐ：／／ｓｅｒｖｉｃｅ．ｒｅｑｕｅｓｔ．ｃｏｍといったＵＲＬをサイトへ発行する。ＵＲＬの発行を受けたサイトはこのＵＲＬを、このＵＲＬの有効期間（受付代行サービスの契約期間）と共に、一般ユーザに公開する。

【００７１】

サービスプロバイダは、顧客であるサイトから具体的なアクセス数やアクセス時間を提示してもらう代わりに、制御情報ＤＢ２１１の処理能力データから最大アクセス許容数を計算して設定するようにシステムを構築することも可能である。この場合の、静的アクセス許容数算出手段２０６が実行する処理のフローチャートを図１５に示す。

【００７２】

図１５において、静的アクセス許容数算出手段２０６は、ステップＳ２０６１でアクセス情報ＤＢ２０９から処理能力データを抽出する。次に、ステップＳ２０６２で抽出した処理能力データから最大アクセス許容数を計算する。この計算式としては、例えば、アクセス情報ＤＢ２０９の処理能力データとして、高速ＣＰＵが搭載されている場合は、受付代行センタで定義されたＣＰＵ対応表等で、１５０％というデータが設定され、大量にメモリを搭載している場合も、同じく受付代行センタの定義された搭載メモリ対応表等で、２００％というデータが設定されると、その平均を取って予め受付代行センタが定義している初期アクセス許容数から以下の計算等で、最大アクセス許容数を算出する。

（初期アクセス許容数）×（１．５＋２．０）／２

最後にステップＳ２０６３で算出した最大アクセス許容数をアクセス情報ＤＢ２０９に設定する。

（２）受付代行サービス開始

サービスプロバイダは、保守コンソールなどを通じて受付代行サービス開始時刻直前に、プロバイダ管理下であるネットワークのエッジルータ、つまり、一般ユーザ用のダイアルアップルータ２１，２２や、他プロバイダと接続する境界ルータにサイトのＩＰアドレス１００．１００．４００．１００へのアクセス規制を設定する。アクセス規制はルータ２１，２２等において、指定されたＩＰアドレスを宛先とするＩＰパケットを棄却する事で行われる。この機能は一般にフィルタリングと呼ばれており、最近の多くのネットワーク装置がこの機能を備えている。設定インタフェースはネットワーク装置により異なるが、ＳＮＭＰや独自のＣＬＩ（コマンドラインインタフェース）が用いられる。

【００７３】

これにより受付代行サービス開始時刻を持って、ユーザは直接ｈｔｔｐ：／／ｓｅｒｖｉｃｅ．ｃｏｍへアクセスできなくなり、このサイトへのアクセスはｈｔｔｐ：／／ｓｅｒｖｉｃｅ．ｒｅｑｕｅｓｔ．ｃｏｍを介したものだけが有効になる。

（３）受付代行センタでの処理概要

ユーザは、ユーザ端末５１，５２よりインターネットブラウザからｈｔｔｐ：／／ｓｅｒｖｉｃｅ．ｒｅｑｕｅｓｔ．ｃｏｍを入力し、受付代行センタへアクセスする。受付代行センタは本発明によらない既存のサーバ負荷分散の仕組みを用いて、負荷分散サーバ群１２０いずれかのサーバにこの要求を回送する。

【００７４】

受付サーバ１００は、既存のアクセス受付手段１１０を介して、ｈｔｔｐプロトコルを受信し、アクセス登録手段１０３にその情報を渡す。アクセス受付手段１１０は、具体的には受付専用のサーバアプリケーションであり、ｈｔｍｌ，Ｊａｖａ，その他のスクリプト言語等で記述される。このアプリケーション自体に、本発明の固有要素は無く、図１６に示すようなアクセス要求情報を抽出し、例えばプロセス間通信を用いてアクセス登録手段１０３に情報を渡す。初回アクセス時、即ちｈｔｔｐ：／／ｓｅｒｖｉｃｅ．ｒｅｑｕｅｓｔ．ｃｏｍへのアクセス時は、要求種別にアクセス要求を設定する。

【００７５】

図１６は、アクセス要求情報のメッセージ構造を示す。アクセス要求情報は、アクセス登録手段１０３に処理指標を示す要求種別（アクセス要求、待合せ応答要求、待合せ拒否要求）、ユーザ端末のＩＰアドレスである送信元ＩＰアドレス、サービスサーバ３００のＩＰアドレスである送信先ＩＰアドレス、サービスサーバ３００がユーザと通信を行うための対象アプリケーションのポート番号である送信先ポート番号からなる。

【００７６】

図１７、図１８はアクセス登録手段１０３の処理を詳細に説明するためのフローチャートを示す。まず、アクセス登録手段１０３は、図１７のステップＳ１０３１で受信したアクセス要求情報の要求種別を判断する。ここでは、アクセス要

求情報の要求種別はアクセス要求であるから、ステップＳ１０３２に分岐する。アクセス要求情報のＩＰアドレスとポート番号でアクセスリスト１０９を索引し、当該アクセスリストの接続状態を示す過負荷フラグを判定する。ここでは過負荷でないものとし、図１８のステップＳ１０３８に分岐する。

【００７７】

ただし、過負荷の場合は、ユーザに待合せを行うことの確認と、予測待合せ時間の通知を行うため、図１７のステップＳ１０３４に分岐する。ユーザに待合せを行うことの確認と、予測待合せ時間の通知については、「受付代行センタでのユーザ通知」で後述する。

【００７８】

ステップＳ１０３８では、抽出したアクセスリスト１０９の優先制御フラグを抽出し、ステップＳ１０３９で優先制御無しか否かを判定する。ここでは優先制御無しが設定されたものとし、ステップＳ１０３１０に分岐する。優先制御ありの場合は、「サービスクラスによる優先制御サービス」で後述する。

【００７９】

ステップＳ１０３１０では図１３に示すアクセスリスト１０９のバッファエリアの空きバッファを検索し、該当バッファに入力されたアクセス要求情報の接続元ＩＰアドレス（１００．１００．２００．１０）を設定し、空きバッファポインタの更新を行う。ステップＳ１０３１１で新たに捕捉したバッファを接続待ちアクセスリスト１０９にキューイングし、ステップＳ１０３１２でアクセスリスト１０９の接続待ちユーザ数を更新する。キューイングの制御については、本発明とは直接関係しないので、説明を省略する。

【００８０】

次に、ステップＳ１０３１３で、図１９に示すフィルタリング要求のフィルタリング要求種別に許可要求を設定し、その他の情報をアクセス要求情報から複写して設定し、フィルタリング最適化手段２０４に制御を渡す。

【００８１】

図１９は、フィルタリング要求のメッセージ構造を示す。フィルタリング要求は、フィルタリング最適化手段２０４に処理指標を示す要求種別（許可要求、不

許可要求、優先制御付き許可要求、アクセス許可を解除するための解除要求）、ユーザ端末のＩＰアドレスである送信元ＩＰアドレス、サービスサーバ３００のＩＰアドレスである送信先ＩＰアドレス、サービスサーバ３００がユーザと通信を行うための対象アプリケーションのポート番号である送信先ポート番号からなる。

【００８２】

図２０、図２１はフィルタリング最適化手段２０４の処理を詳細に説明するためのフローチャートを示す。この処理は、実際にはアクセス情報ＤＢ２０９に登録された全インスタンスについて実行されるが、ここでは説明を簡単にするために１インスタンスの処理のみを記述する。

【００８３】

まず、フィルタリング最適化手段２０４は、図２０のステップＳ２０４１で入力されたフィルタリング要求のフィルタリング要求種別を判定する。フィルタリング要求種別が許可要求であれば、ステップＳ２０４２に分岐する。優先制御付き許可要求であれば、ユーザクラス別にアクセス要求を読み出す。ユーザクラス別にアクセス要求を読み出す手段については、「サービスクラスによる優先制御サービス」で後述する。

【００８４】

ステップＳ２０４２ではアクセス情報ＤＢ２０９よりポート番号対応に最大アクセス許容数を抽出する。次に、ステップＳ２０４３でアクセスリスト１０９より過負荷フラグを抽出し、ステップＳ２０４４で過負荷フラグを判定し、接続空き無しであれば処理を終了する。

【００８５】

過負荷フラグが接続空き有りの場合は、ステップＳ２０４５でアクセスリスト１０９の接続中ユーザ数を抽出し、ステップＳ２０４６で最大アクセス許容数から接続中ユーザ数を差し引いた分、接続待ちアクセスリスト１０９から送信元ＩＰアドレスを抽出し、内部データの新規アクセス許可リストに設定する。新規アクセス許可リストは、接続待ちアクセスリスト１０９から抽出した送信元ＩＰアドレスで構成される。この後、ステップＳ２０４７で有効タイマ設定手段２０３

を起動してステップＳ２０４１２に進む。有効タイマ設定手段２０３については後述する。

【００８６】

図２１のステップＳ２０４１２では、内部データの新規アクセス許可リストが無くなるまでループ処理を行う。ステップＳ２０４８では、アクセス情報ＤＢ２０９よりアクセス許可対象ＩＰアドレスに対するネットワーク装置のＩＰアドレスとパケットフィルタリング機能種別を抽出する。そして、ステップＳ２０４９でパケットフィルタリング機能種別に対応した許可フィルタリング・コマンドを作成する。ステップＳ２０４１０で、作成した許可フィルタリング・コマンドと、ステップＳ２０４８で抽出したネットワーク装置のＩＰアドレスとを図２２に示すフィルタリング・コマンド実行要求に設定し、トラヒック制御手段２１０に制御を渡す。そして、ステップＳ２０４１３で処理済みアクセス許可対象ＩＰアドレスを削除する。

【００８７】

図２２は、フィルタリング・コマンド実行要求のメッセージ構造を示す。フィルタリング・コマンド実行要求は、フィルタリングを実行するネットワーク装置のＩＰアドレスとフィルタリング・コマンドフィールドからなる。フィルタリング・コマンドフィールドは、例えばユーザ端末５１（１００．１００．２００．１０）からサービスサーバ３００（１００．１００．４００．１００）にWWW（ｈｔｔｐ）でのアクセスを不許可にする場合は、「ｉｐｃｈａｉｎｓ　－ｓ　１００．１００．２００．１０　－ｄ　１００．１００．４００．１００　－ｐ　ｈｔｔｐ　－ｊ　ＤＥＮＹ」という実行可能レベルのコマンドが設定されている。

【００８８】

図２３は、トラヒック制御手段２１０の処理を詳細に説明するためのフローチャートを示す。まず、トラヒック制御手段２１０は、ステップＳ２１０１で入力されたフィルタリング・コマンド実行要求のＩＰアドレスに対して、Ｔｅｌｎｅｔ等を用いて通信ポートを開く。次に、ステップＳ２１０２で開いた通信ポートを介し、入力されたフィルタリング・コマンド実行要求のフィルタリング・コマ

ンドを起動する。ここでは、許可フィルタリング・コマンドを起動することで、ユーザは直接ｈｔｔｐ：：／／ｓｅｒｖｉｃｅ．ｃｏｍに対しアクセス可能となる。

（４）受付代行センタでのアクセス許可解除

ここでは、直接ｈｔｔｐ：：／／ｓｅｒｖｉｃｅ．ｃｏｍにアクセス可能となったユーザのアクセス許可を解除する実施例を示す。

【００８９】

受付代行センタは、アクセス許可を解除する手段として、サービスサーバ３００へのアクセス有効タイマが満了した時に解除する手段と、サービスサーバ３００とユーザとのサービス・セッション、例えば、ユーザが購入した動画データをダウンロードするセッション、インターネット・ショッピングにおける購入手続きのセッション、が終了した時にサービスサーバ３００から受付代行センタへサービス・セッションが終了したことを通知することによる解除手段とを備えている。

【００９０】

サービスサーバ３００へのアクセス有効タイマ満了による解除手段は、フィルタリング最適化手段２０４の処理の中で起動する有効タイマ設定手段２０３であり、有効タイマ値をアクセスリスト１０９に設定する。

【００９１】

図２４は、有効タイマ設定手段２０３の処理を詳細に説明するためのフローチャートを示す。まず、有効タイマ設定手段２０３は、ステップＳ２０３１でアクセス情報ＤＢ２０９より入力された有効タイマ設定要求の送信先ＩＰアドレスと送信先ポート番号に対する有効タイマ値を抽出する。次に、ステップＳ２０３２で入力された有効タイマ設定要求の要求種別が優先制御有りか、無しかを判定する。ここでは優先制御無しが設定されているものとし、ステップＳ２０３３に分岐する。

【００９２】

ステップＳ２０３３では、入力された有効タイマ設定要求の最大アクセス許容数と接続中ユーザ数の差分分を待合せアクセスリスト１０９から接続中アクセス

リスト１０９にキューを移す。ステップＳ２０３４で先のステップＳ２０３１で抽出した有効タイマ値を、現時刻に加算する。ステップＳ２０３５では接続中アクセスリスト１０９に移されたキューが持つ有効タイマ値に、先のステップＳ２０３４で算出された値を設定する。

【００９３】

例えば、アクセス情報ＤＢ２０９から抽出した有効タイマ値が７分で、現時刻が７時３０分ならば、７時３７分となり、サービスサーバ３００へのアクセス許可が解除される時刻が７時３７分ということを示す。次に、ステップＳ２０３６で上記解除される時刻が設定されたバッファ・エリアをアクセスリスト１０９の有効タイマ順ポインタにキューイングする。そして、ステップＳ２０３７でアクセス情報ＤＢ２０９の入力された有効タイマ設定要求の送信先ＩＰアドレスと送信先ポート番号に対する接続中ユーザ数を加算して、接続待ちユーザ数を減算する。

【００９４】

有効タイマ手段２０３によってユーザがサービスサーバ３００へアクセスするアクセス可能な時間が設定されるので、フィルタリング解除手段２０２はアクセス可能な時間が満了していないかを周期的に確認を行い、アクセス可能な時間が満了していた場合は、ユーザのサービスサーバ３００へのアクセス許可を解除する。

【００９５】

図２５は、フィルタリング解除手段２０２の処理を詳細に説明するためのフローチャートを示す。フィルタリング解除手段２０２は、ある一定の周期でシステムを構築したＯＳ（オペレーション・システム）が持つタイマ起動で呼び出される。まず、ステップＳ２０２１でアクセスリスト１０９の有効タイマ順ポインタによりキューイングされたキューから有効タイマ切れの送信元ＩＰアドレスを抽出し、ステップＳ２０２２でアクセスリスト１０９の有効タイマ順ポインタによりキューイングされたキューから上記抽出した分を削除する。

【００９６】

次に、ステップＳ２０２３でアクセス情報ＤＢ２０９より先のステップＳ２０

２１で抽出したアクセス解除対象のＩＰアドレスに対するネットワーク装置のＩＰアドレスとパケットフィルタリング機能種別を抽出する。そして、ステップＳ２０２４でアクセスリスト１０９の有効タイマ順ポインタによりキューイングされたキューから先のステップＳ２０２１で抽出した分を、接続中アクセスリスト１０９から空きバッファ・キューに移し、接続中ユーザ数を減算する。

【００９７】

次に、ステップＳ２０２５でパケットフィルタリング機能種別に対応したアクセス許可を解除するフィルタリング・コマンドを作成し、ステップＳ２０２６で作成した解除フィルタリング・コマンドと、先のステップＳ２０２３で抽出したネットワーク装置のＩＰアドレスとを図２２に示すフィルタリング・コマンド実行要求に設定し、トラヒック制御手段２１０に制御を渡す。トラヒック制御手段２１０によってアクセス許可を解除するフィルタリング・コマンドを起動することで、ユーザは直接ｈｔｔｐ：／／ｓｅｒｖｉｃｅ．ｃｏｍへアクセスが出来なくなる。

【００９８】

次に、受付代行センタが備えるもう一つの解除手段、サービスサーバ３００とユーザとのサービス・セッションが終了した時にサービスサーバ３００から受付代行センタへサービス・セッションが終了したことを通知することによる解除手段を説明する。

【００９９】

サービスサーバ３００は、例えば、ユーザが購入した動画データをダウンロードするセッション、インターネット・ショッピングにおける購入手続きのセッションのような通信を途中で切断されて困る場合は、サービスプロバイダと受付代行サービスを契約する際に、提示する自サイトのサーバ処理能力を示す一人当たりの平均アクセス時間を長く設定しておき、周期的にアクセス解除する手段に頼らず、サービスサーバ３００が図２６のセッション終了通知手段３０１によりアクセス解除する手段を利用できる。

【０１００】

図２６は、セッション終了通知手段３０１の処理を詳細に説明するためのフロ

ーチャートを示す。サービスサーバ３００は、既存のセッション終了判定手段３０２を用いてセッション終了を判定し、図２７に示すセッション終了通知メッセージのサービスサーバ３００ＩＰアドレスに自ＩＰアドレス、サービスサーバ３００ポート番号に、ユーザとのセッションに使用したポート番号、クライアントＩＰアドレスにセッションを行ったユーザのＩＰアドレスを設定し、セッション終了通知手段３０１を起動する。これにより、セッション終了通知手段３０１は、図２６のステップＳ３０１１でアクセス制御サーバのセッション完了フィルタリング解除手段２０８に入力されたセッション終了通知を送信する。

【０１０１】

図２７は、セッション終了通知のメッセージ構造を示す。セッション終了通知は、サービスサーバ３００のＩＰアドレスであるサービスサーバＩＰアドレス、ユーザとのセッションに使用したポート番号であるサービスサーバポート番号、セッションを行ったユーザのＩＰアドレスであるクライアントＩＰアドレスからなる。

【０１０２】

図２８は、セッション完了フィルタリング解除手段２０８の処理を詳細に説明するためのフローチャートを示す。セッション完了フィルタリング解除手段２０８は、サービスサーバ３００からのセッション終了通知を受けるべく、ある通信ポートを開いてメッセージ受信待ちとなっている。まず、ステップＳ２０８１でアクセス情報ＤＢ２０９より入力されたセッション終了通知のクライアントＩＰアドレスに対するネットワーク装置のＩＰアドレスとパケットフィルタリング機能種別を抽出する。そして、ステップＳ２０８２でアクセスリスト１０９から入力されたセッション終了通知のサービスサーバ３００のＩＰアドレス、サービスサーバ３００ポート番号、クライアントＩＰアドレスに対するアクセス許可解除対象のバッファ・エリアを接続中アクセスリスト１０９のキューから空きバッファのキューに変更し、接続中ユーザ数を減算する。

【０１０３】

次に、ステップＳ２０８３でパケットフィルタリング機能種別に対応したアクセス許可を解除するフィルタリング・コマンドを作成する。次に、ステップＳ２

０８４で作成した解除フィルタリング・コマンドと、先のステップＳ２０８１で抽出したネットワーク装置のＩＰアドレスとを図２２に示すフィルタリング・コマンド実行要求に設定し、トラヒック制御手段２１０に制御を渡す。これにより、トラヒック制御手段２１０によってアクセス許可を解除するフィルタリング・コマンドを起動することで、ユーザは直接ｈｔｔｐ：／／ｓｅｒｖｉｃｅ．ｃｏｍへアクセスが出来なくなる。

（５）受付代行センタでのユーザ通知

受付代行センタはユーザに対して待合せを行うことの確認、及び予測待合せ時間の通知を、サービスサーバ３００が過負荷か否かを判断し（図１７のステップＳ１０３３）、過負荷の場合には、アクセスリスト１０９に登録する処理の前に行う。

【０１０４】

最初に待合せを行うことをユーザに確認する手段について説明する。図２９は、アクセス確認手段１０４の処理を詳細に説明するためのフローチャートを示す。図３０は、待合せ確認通知手段１０５の処理を詳細に説明するためのフローチャートを示す。ユーザは、ユーザ端末よりサービスサーバ３００へのアクセス要求を受付サーバ１００のアクセス受付手段１１０に送信する。アクセス受付手段１１０は、受信したアクセス要求をアクセスリスト１０９に登録するようアクセス登録手段１０３に要求する。アクセス登録手段１０３は、アクセス要求情報をアクセスリスト１０９に登録するか否かを確認する場合（過負荷の場合：図１７のステップＳ１０３３で判断する）、アクセス確認手段１０４にアクセスリスト登録確認を行う。

【０１０５】

アクセス確認手段１０４は、図２９のステップＳ１０４１において、アクセス確認を行うための確認メッセージを作成する。次に、ステップＳ１０４２で作成した確認メッセージを待合せ確認通知手段１０５に処理を渡す。待合せ確認通知手段１０５は、図３０のステップＳ１０５１において、確認メッセージをＨＴＴＰプロトコルでユーザに通知する。そして、ユーザは確認メッセージの応答をアクセス受付手段１１０に再度送信する。アクセス受付手段１１０は、ユーザから

の応答をアクセス登録手段１０３に送信し、アクセス登録手段１０３はユーザからの応答が登録ならば（図１７のステップＳ１０３１で判断する）、アクセスリスト１０９にアクセス要求情報を登録する。

【０１０６】

次に予測待合せ時間を通知する手段を説明する。図３１は、予測待合時間算出手段１０６の処理を詳細に説明するためのフローチャートを示す。図３２は、アクセス情報通知手段１０７の処理を詳細に説明するためのフローチャートを示す。ユーザは、ユーザ端末よりサービスサーバ３００へのアクセス要求を受付サーバ１００のアクセス受付手段１１０に送信する。アクセス受付手段１１０は、受信したアクセス要求をアクセスリスト１０９に登録するようアクセス登録手段１０３に要求する。アクセス登録手段１０３は、空きのアクセスリスト１０９がない過負荷の場合（図１７のＳ１０３３で判断する）、予測待合時間算出手段１０６へ予約待合時間算出要求をする。

【０１０７】

予測待合時間算出手段１０６は、図３１のステップＳ１０６１において、アクセスリスト１０９より入力されたアクセス要求情報の送信先ＩＰアドレスと送信先ポート番号に対する待合せアクセスリスト１０９のユーザ数と有効タイマ値を抽出し、有効タイマ値とユーザ数の乗算を行い待合せ時間を算出し、ステップＳ１０６２で予測待合せ時間を通知するメッセージを作成する。そして、ステップＳ１０６３で作成した予測待合せ時間を通知するメッセージをアクセス情報通知手段１０７に処理を渡す。アクセス情報通知手段１０７は、図３２のステップＳ１０７１で予測待合せ時間を通知するメッセージをＨＴＴＰプロトコルでユーザに通知する。

【０１０８】

Ｂ．インターネットサービスプロバイダによる最適アクセスサービス

また、本発明は、前述の図１５を用いて説明した静的アクセス許容数算出手段２０６だけでなく、図３３の動的アクセス許容数算出手段２０７によって、サーバのＣＰＵ使用率、ネットワーク使用率を考慮してサービスサーバ３００への最大アクセス許容数を動的に変更する。

【０１０９】

図３３は、動的アクセス許容数算出手段２０７の処理を詳細に説明するためのフローチャートを示す。以下、既存の負荷・トラヒック監視装置２１２用いて、周期的にサービスサーバ３００の負荷状態、及びサービスサーバ３００を収容するネットワーク装置のトラフィック状態の情報を抽出し、最大アクセス許容数を変更することで、実際の処理負荷やネットワークのトラヒックに対するアクセスを許容可能とする手段について説明する。

図３３において、動的アクセス許容数算出手段２０７は、ステップＳ２０７１で周期的に負荷・トラヒック監視装置２１２からサービスサーバ３００の負荷状態、及びサービスサーバ３００を収容するネットワーク装置のトラフィック状態の情報を抽出し、各データの平均値を算出する。例えば、ＣＰＵ使用率８０％、トラヒック量がサーバ・許容トラヒック量（ワイヤ・スピード）に対しての使用量９０％の場合、平均値は８５％となる。

【０１１０】

ステップＳ２０７２ではアクセス情報ＤＢ２０９から現在設定されている最大アクセス許容数を抽出し、現在のＣＰＵ使用量、及びトラヒック量にあった最大アクセス許容数を算出する。本発明はその算出方法については特定しないが、例えば、ステップＳ２０７１で算出された平均値が８５％であれば、その算出方法は、８０％以上の場合だけ変更を行い、以下の計算を行う。

（抽出した最大アクセス許容数）×［１－（０．８５－０．８）］

そして、ステップＳ２０７３で、その最大アクセス許容数をアクセス情報ＤＢ２０９に設定する。

【０１１１】

Ｃ．インターネットサービスプロバイダによるサービスクラスによる優先制御サービス

前記Ａ（１）の受付代行サービスの契約時に契約するサービスサーバ３００がユーザクラスによる優先制御を行うかどうかをサービスサーバ３００の契約者は選択できる。優先制御を行う場合は、アクセスリスト１０９内の優先制御の有無を示す優先制御フラグを優先制御ありを示すフラグを設定しておくことで、サー

ビスサーバ３００へのアクセス許可が高優先のユーザから優先的に許可可能となる。

【０１１２】

前記Ａ（３）で説明したアクセス登録手段１０３は、サービスサーバ３００が優先制御ありかどうかを判断し、優先制御ありならば、図３４に示すユーザクラス別アクセス登録手段１０８で、ユーザクラス別にアクセスリスト１０９にアクセス要求情報を登録する。

【０１１３】

図３４は、ユーザクラス別アクセス登録手段１０８の処理を詳細に説明するためのフローチャートを示す。ユーザクラス別アクセス登録手段１０８は、ステップＳ１０８１でユーザプロファイル１１１から図３５（Ａ）に示す処理手順のユーザクラス抽出手段１０２を用いてユーザクラスを抽出する。ここでは、図３５（Ｂ）に示すように、入力されたアクセス要求情報の送信元ＩＰアドレスを用いてユーザプロファイル１１１を検索してユーザクラスを抽出する。

【０１１４】

次に、ステップＳ１０８２でバッファエリアの空きバッファキューを検索し、該当バッファに接続元ＩＰアドレスを設定し、バッファエリアの空きバッファキューを更新し、ステップＳ１０８３で新たに捕捉したバッファを接続待ちアクセスリスト１０９にキューイングする。そして、ステップＳ１０８４でアクセスリスト１０９の接続待ちユーザ数を加算する。キューイングの制御については、本発明とは直接関係しないので説明を省略する。その後、ステップＳ１０８５で、図１９に示すフィルタリング要求のフィルタリング要求種別に優先制御付き許可要求を、その他の情報をアクセス要求情報から複写して設定、フィルタリング最適化手段２０４に制御を渡す。

【０１１５】

これにより、フィルタリング最適化手段２０４は、アクセスリスト１０９から最大アクセス許容数分のアクセス情報を読み出す際に、入力されたフィルタリング要求のフィルタリング要求種別を判断し（図２０のステップＳ２０４１）、優先制御付き許可要求の場合、ユーザクラス別アクセス要求読出手段２０５を起動

する（図２０のステップＳ２０４１１）。そして、出力されたＩＰアドレスを内部データ新規アクセス許可リストに設定する。

【０１１６】

図３６は、ユーザクラス別アクセス要求読出手段２０５の処理を詳細に説明するためのフローチャートを示す。ユーザクラス別アクセス要求読出手段２０５は、ステップＳ２０５１でアクセス情報ＤＢ２０９より送信先ＩＰアドレスと送信先ポート番号対する最大アクセス許容数を抽出する。次に、ステップＳ２０５２でアクセスリスト１０９より過負荷フラグを抽出する。そして、ステップＳ２０５４で過負荷フラグを判定し、接続空き無しであれば処理を終了する。接続空き有りであればステップＳ２０５３に分岐する。

【０１１７】

ステップＳ２０５３では、制御情報ＤＢ２１１から入力されたフィルタリング要求の送信先ＩＰアドレスと送信先ポート番号に対する読出比率を抽出する。例えば、読出比率が３：２：１ならば、高優先リストから割合１／２で、中優先リストから１／３で、低優先リストから１／６の比率でアクセス要求情報をアクセスリスト１０９から読み出すことを示す。

【０１１８】

次に、ステップＳ２０５５で入力されたフィルタリング要求の送信先ＩＰアドレスと送信先ポート番号に対する各ユーザクラスの接続中ユーザ数を抽出する。ステップＳ２０５６で先にステップＳ２０５３で抽出した読出比率でアクセスリスト１０９からアクセス要求情報を読み出し、ステップＳ２０５７で有効タイマ設定手段２０３を起動する。そして、抽出したアクセス要求情報の送信元ＩＰアドレスを呼び元に返す。このようにして、ユーザクラス別にアクセス要求情報をアクセスリスト１０９から抽出する。

【０１１９】

図３７は、有効タイマ設定要求のメッセージ構造を示す。有効タイマ設定要求は、優先制御ありか否かを示す要求種別、最大アクセス許容数と接続中ユーザとの差分、サービスサーバ３００のＩＰアドレスである送信先ＩＰアドレス、サービスサーバ３００がユーザと通信を行うための対象アプリケーションのポート番

号である送信先ポート番号からなる。最大アクセス許容数と接続中ユーザとの差分は、優先制御なしの場合は、データは１つであるが、優先制御ありの場合、ユーザクラスの種類分データが設定されている。例えば、高優先、中優先、低優先の場合は、３つのデータが設定されている。

【０１２０】

Ｄ．インターネットサービスプロバイダによる不許可ユーザ規制サービス

前述のＡ（１）の受付代行サービスの契約で説明したように、サービスプロバイダは、サービスを提供するサービスサーバ３００に例えば、ｈｔｔｐ：／／ｓｅｒｖｉｃｅ．ｒｅｑｕｅｓｔ．ｃｏｍといったＵＲＬをサイトへ発行する。そして、ＵＲＬの発行を受けたサイトはこのＵＲＬを、このＵＲＬの有効期間（受付代行サービスの契約期間）と共に、一般ユーザへ公開する。

【０１２１】

サービスを提供するサーバは、ＵＲＬ公開の前にユーザとのサービス契約を結び、そのユーザからのアクセスのみをユーザプロファイル１１１にアクセス許可として登録し、契約していないユーザに対しては不許可ユーザとして登録することが可能である。ユーザプロファイル１１１に登録された不許可ユーザからのアクセスは、サービスサーバ３００の代わりに受付代理センタがユーザ認証を行い、不許可ユーザからサービスサーバ３００へアクセスを未然に防止することで、サービスサーバ３００に余分な負荷を及ぼさない。

【０１２２】

ユーザ端末よりサービスサーバ３００へのアクセス要求があると、アクセス受付手段１１０は、ユーザ認証手段１０１へアクセス要求情報を通知する。

【０１２３】

図３８は、ユーザ認証手段１０１の処理を詳細に説明するためのフローチャートを示す。また、図３９はアクセス不許可フィルタリング設定手段２０１の処理を詳細に説明するためのフローチャートを示す。

【０１２４】

ユーザ認証手段１０１は、図３８のステップＳ１０１０で入力されたアクセス要求情報の要求種別を判定し、要求種別がアクセス要求であればステップＳ１０

１１に分岐し、アクセス要求で無ければステップＳ１０１５でアクセス要求情報をアクセス登録手段１０３に引き渡す。

【０１２５】

ステップＳ１０１１では、アクセス要求情報の送信元ＩＰアドレスのユーザクラスをユーザプロファイル１１１からユーザクラス抽出手段１０２を介してユーザクラスを抽出する。そして、ステップＳ１０１２で抽出したユーザクラスを判定し、アクセス不許可の場合は、ステップＳ１０１３に分岐してフィルタリング要求種別を不許可とするフィルタリング要求を、アクセス不許可フィルタリング設定手段２０１に引き渡す。一方、アクセス許可の場合は、ステップＳ１０１４でアクセス要求情報をアクセス登録手段１０３に引き渡す。

【０１２６】

図２０において、アクセス不許可フィルタリング設定手段２０１は、ステップＳ２０１１でアクセス情報ＤＢ２０９より入力されたフィルタリング要求の送信先ＩＰアドレスに対するネットワーク装置のＩＰアドレスとパケットフィルタリング機能種別を抽出し、ステップＳ２０１２でパケットフィルタリング機能種別に対応した不許可フィルタリング・コマンドを作成する。ステップＳ２０１３では、作成した不許可フィルタリング・コマンドと、先のステップＳ２０１１で抽出したネットワーク装置のＩＰアドレスとを図２２に示すフィルタリング・コマンド実行要求に設定し、トラヒック制御手段２１０に制御を渡す。このトラヒック制御手段２１０によって不許可フィルタリング・コマンドを起動することで、ユーザは直接ｈｔｔｐ：：／／ｓｅｒｖｉｃｅ．ｃｏｍへアクセスが出来なくなる。

【０１２７】

本発明においては、常時、サーバの能力を効果的に引き出すためにサービスサーバ３００が処理可能な分のユーザがサービスサーバ３００に直接アクセスする方法をとっているので、プロキシー・サーバのキャッシュ機能を用いた際に発生するコンテンツが更新されない課題や、アクセスする度に内容が変化する動的オブジェクトが再利用できないという課題が解決されると共に、無意味なトラヒックがコアネットワーク１０に流さないため、トラヒックの軽減も図ることができ

る。さらに、トラヒック量を軽減することにより、ネットワーク・リソースの有効活用も可能とする。

【０１２８】

本発明においては、ユーザからのアクセス要求の待合せを可能としており、サービスサーバ３００で接続コネクション数を設定した場合に比べてユーザに与える負担も軽減される。さらに、本発明ではサービスサーバ３００の負荷状況やトラヒック状況を定期的に監視しているので、接続先のサービスサーバ３００の処理能力を把握でき、サービスサーバ３００が最適に動作可能なアクセス分のユーザにアクセスを許可することが可能となる。

【０１２９】

さらに、現状では、ユーザが高トラヒック、または過負荷なサービスサーバにアクセスした場合、応答速度が遅かったり、散々応答を待った挙げ句アクセスを拒否する旨のメッセージが送信されるという問題があるが、本発明を適用すると待合せが可能であるため、アクセス要求したユーザは自分のアクセス順番になれば、速い応答速度で快適にサービスを受けることが可能となる。

【０１３０】

さらに、本発明が必要となるような接続要求輻輳時に本発明によるアクセス制御を行い、非輻輳状態においては、従来技術による通常接続制御を行う、というように常に最良の接続性を保証することも可能である。

【０１３１】

（付記１）　パケットフィルタリング機能を有するネットワーク装置と、

前記ネットワーク装置を介してＩＰネットワークに接続され、ユーザにサービスを提供するサービスサーバと、

前記ネットワーク装置を介してＩＰネットワークに接続されサービスサーバが提供するサービスを利用するためのユーザ端末と、

前記ＩＰネットワークに接続されサービスサーバの受付としてユーザ端末からのアクセスを受け付ける受付サーバと、

前記ネットワーク装置を制御するアクセス制御サーバと、で構成されるネットワークシステムのネットワークアクセス制御方法において、

前記受付サーバは、ユーザ端末からのアクセス要求情報を受信して保持し、

前記アクセス制御サーバは、前記サービスサーバの処理能力及びサービスサーバへのトラヒック量に基づき最適に処理可能なアクセス要求分だけ前記アクセス登録手段に保持されたアクセス要求情報を抽出して前記サービスサーバへのアクセスを許容するトラヒック制御を行うことを特徴とするネットワークアクセス制御方法。

【０１３２】

（付記２）　パケットフィルタリング機能を有するネットワーク装置と、

前記ネットワーク装置を介してＩＰネットワークに接続され、ユーザにサービスを提供するサービスサーバと、

前記ネットワーク装置を介してＩＰネットワークに接続されサービスサーバが提供するサービスを利用するためのユーザ端末と、

前記ＩＰネットワークに接続されサービスサーバの受付としてユーザ端末からのアクセスを受け付けるアクセス受付手段を備えた受付サーバと、

前記ネットワーク装置を制御するトラヒック制御手段を備えたアクセス制御サーバと、で構成されるネットワークシステムにおいて、

前記受付サーバは、前記アクセス受付手段を介しユーザ端末からのアクセス要求情報を受信して保持するアクセス登録手段を有し、

前記アクセス制御サーバは、前記サービスサーバの処理能力及びサービスサーバへのトラヒック量に基づき最適に処理可能なアクセス要求分だけ前記アクセス登録手段に保持されたアクセス要求情報を抽出して前記サービスサーバへのアクセスを許容するトラヒック制御を行うフィルタリング最適化手段を有することを特徴とするネットワークシステム。

【０１３３】

（付記３）　ユーザ端末からのアクセス要求情報を保持するアクセスリストと、

各ユーザのユーザクラスを含むユーザ情報を保持するユーザプロファイルと、

ユーザ端末からのアクセスを受け付けるアクセス受付手段と、

前記アクセス受付手段を介し受信したアクセス要求情報を前記アクセスリスト

に受付順に登録するアクセス登録手段と、

受信したアクセス要求情報からＩＰアドレスを抽出し、ＩＰアドレスによりユーザを特定して前記ユーザプロファイルからユーザクラスを抽出するユーザクラス抽出手段と、

前記アクセス受付手段を介し受信したアクセス要求情報を前記ユーザクラス抽出手段で抽出したユーザクラスに基づいて前記アクセスリストに登録するユーザクラス別アクセス登録手段を

有することを特徴とする受付サーバ。

【０１３４】

（付記４）　付記３記載の受付サーバにおいて、

ユーザ端末からのアクセス要求を受け付けて前記アクセスリストへ登録する位置に応じた待ち合わせを行っているユーザ数から予測待ち合わせ時間を算出する予測待合時間算出手段と、

算出した予測待ち合わせ時間の情報をユーザに通知し予測待ち合わせ時間経過後、ユーザ端末にアクセス可能であることを通知するアクセス情報通知手段を

有することを特徴とする受付サーバ。

【０１３５】

（付記５）　付記３記載の受付サーバにおいて、

ユーザ端末からのアクセス要求を受け付けた際に、待ち合わせが必要な場合、前記アクセス要求をアクセスリストに登録するか否かをユーザ端末に確認するアクセス確認手段と、

前記アクセス確認手段の確認をユーザ端末に通知する待合せ確認通知手段を

有することを特徴とする受付サーバ。

【０１３６】

（付記６）　サービスサーバの処理能力に関する情報及びサービスサーバの処理能力に基づき算出された最大アクセス許容数を保持するアクセス情報データベースと、

ネットワーク装置を制御するトラヒック制御手段と、

前記サービスサーバの処理能力に関する情報に基づき最大アクセス許容数を算

出する静的アクセス許容数算出手段と、

受付サーバでユーザ端末からのアクセス要求情報を保持するアクセスリストの先頭から最大アクセス許容数分のアクセス要求情報を読み出し、アクセス要求を行ったユーザ端末をサービスサーバにアクセス可能とするパケットフィルタリング設定情報を生成し前記トラヒック制御手段を介して前記ネットワーク装置に設定するフィルタリング最適化手段を

有することを特徴とするアクセス制御サーバ。

【０１３７】

（付記７）　付記６記載のアクセス制御サーバにおいて、

前記サービスサーバの負荷状態及びサービスサーバを収容するネットワーク装置のトラフィック状態を監視する負荷・トラヒック監視装置と、

周期的に負荷・トラヒック監視装置と通信して前記負荷状態及びトラヒック状態の情報を抽出して前記アクセス情報データベースの最大アクセス許容数を算出すると共に、算出した最大アクセス許容数を前記アクセス情報データベースに登録する動的アクセス許容数算出手段を

有することを特徴とするアクセス制御サーバ。

【０１３８】

（付記８）　付記６記載のアクセス制御サーバにおいて、

ユーザ端末からのアクセス要求情報を前記アクセスリストから読み出す際に読み出す指針となる制御情報を保持する制御情報データベースと、

前記フィルタリング最適化手段が前記アクセスリストから最大アクセス許容数分のアクセス要求情報を読み出す際に前記アクセスリストがユーザクラス別に登録されている場合、前記制御情報データベースから抽出された制御情報に基づき前記アクセスリストの各ユーザクラスからアクセス要求情報を読み出すユーザクラス別アクセス要求読出手段を

有することを特徴とするアクセス制御サーバ。

【０１３９】

（付記９）　付記６記載のアクセス制御サーバにおいて、

パケットフィルタリング設定情報を生成する際にアクセス要求情報に有効タイ

マを設定する有効タイマ設定手段と、

前記有効タイマの満了時にネットワーク装置に設定したパケットフィルタリング制御を解除するフィルタリング解除手段を

有することを特徴とするアクセス制御サーバ。

【０１４０】

（付記１０）　ネットワーク装置を介してＩＰネットワークに接続され、ユーザにサービスを提供するサービスサーバにおいて、

ユーザ端末とのセッションを終了したこと判定するセッション終了判定手段と、

前記ユーザ端末とのセッションを終了したことをアクセス制御サーバに通知するセッション終了通知手段を

有することを特徴とするサービスサーバ。

【０１４１】

（付記１１）　付記３記載の受付サーバにおいて、

前記ユーザクラス抽出手段で抽出したユーザクラスに基づき前記アクセス受付手段を介し受信したアクセス要求が不許可のユーザからか否かを判定し、不許可ユーザであればアクセス制御サーバにその旨を通知するユーザ認証手段を

有することを特徴とする受付サーバ。

【０１４２】

（付記１２）　付記６記載のアクセス制御サーバにおいて、

付記１１記載の受付サーバのユーザ認証手段からの通知に基づき前記サービスサーバにアクセス不許可とするパケットフィルタリング設定情報を生成して前記ネットワーク装置に設定するアクセス不許可フィルタリング設定手段を

有することを特徴とするアクセス制御サーバ。

【０１４３】

【発明の効果】

上述の如く、請求項１に記載の発明は、受付サーバは、ユーザ端末からのアクセス要求情報を受信して保持し、アクセス制御サーバは、サービスサーバの処理能力及びサービスサーバへのトラヒック量に基づき最適に処理可能なアクセス要求

分だけアクセス登録手段に保持されたアクセス要求情報を抽出して前記サービスサーバへのアクセスを許容するトラヒック制御を行うため、ユーザがサービスサーバにアクセスする場合に、サービスサーバの処理能力及びサービスサーバへのトラヒック量に見合う分だけのユーザからのアクセスが許容され、動的オブジェクトを再利用できると共にトラヒックの軽減を図ることができる。

【０１４４】

請求項２に記載の発明は、受付サーバは、アクセス受付手段を介しユーザ端末からのアクセス要求情報を受信して保持するアクセス登録手段を有し、アクセス制御サーバは、前記サービスサーバの処理能力及びサービスサーバへのトラヒック量に基づき最適に処理可能なアクセス要求分だけアクセス登録手段に保持されたアクセス要求情報を抽出して前記サービスサーバへのアクセスを許容するトラヒック制御を行うフィルタリング最適化手段を有するため、ユーザがサービスサーバにアクセスする場合に、サービスサーバの処理能力及びサービスサーバへのトラヒック量に見合う分だけのユーザからのアクセスが許容され、動的オブジェクトを再利用できると共にトラヒックの軽減を図ることができる。

【０１４５】

請求項３に記載の発明は、ユーザ端末からのアクセス要求情報を保持するアクセスリストと、各ユーザのユーザクラスを含むユーザ情報を保持するユーザプロファイルと、ユーザ端末からのアクセスを受け付けるアクセス受付手段と、アクセス受付手段を介し受信したアクセス要求情報を前記アクセスリストに受付順に登録するアクセス登録手段と、受信したアクセス要求情報からＩＰアドレスを抽出し、ＩＰアドレスによりユーザを特定して前記ユーザプロファイルからユーザクラスを抽出するユーザクラス抽出手段と、アクセス受付手段を介し受信したアクセス要求情報を前記ユーザクラス抽出手段で抽出したユーザクラスに基づいて前記アクセスリストに登録するユーザクラス別アクセス登録手段を有するため、ユーザクラス別にユーザからのアクセス要求情報を登録することができる。

【０１４６】

請求項４に記載の発明は、ユーザ端末からのアクセス要求を受け付けて前記アクセスリストへ登録する位置に応じた待ち合わせを行っているユーザ数から予測

待ち合わせ時間を算出する予測待合時間算出手段と、算出した予測待ち合わせ時間の情報をユーザに通知し予測待ち合わせ時間経過後、ユーザ端末にアクセス可能であることを通知するアクセス情報通知手段を有するため、ユーザにサービスへのアクセス可能となるまでの時間を通知してユーザからのアクセス要求の待合せを可能とし、ユーザに与える負担を軽減できる。

【０１４７】

請求項５に記載の発明は、ユーザ端末からのアクセス要求を受け付けた際に、待ち合わせが必要な場合、前記アクセス要求をアクセスリストに登録するか否かをユーザ端末に確認するアクセス確認手段と、アクセス確認手段の確認をユーザ端末に通知する待合せ確認通知手段を有するため、ユーザに待合せを行うことを確認することができる。

【０１４８】

付記６に記載の発明は、サービスサーバの処理能力に関する情報及びサービスサーバの処理能力に基づき算出された最大アクセス許容数を保持するアクセス情報データベースと、ネットワーク装置を制御するトラヒック制御手段と、サービスサーバの処理能力に関する情報に基づき最大アクセス許容数を算出する静的アクセス許容数算出手段と、受付サーバでユーザ端末からのアクセス要求情報を保持するアクセスリストの先頭から最大アクセス許容数分のアクセス要求情報を読み出し、アクセス要求を行ったユーザ端末をサービスサーバにアクセス可能とするパケットフィルタリング設定情報を生成し前記トラヒック制御手段を介して前記ネットワーク装置に設定するフィルタリング最適化手段を有するため、サービスサーバの処理能力に見合うユーザからのアクセスを受け付ける制御を行うことができる。

【０１４９】

付記７に記載の発明は、サービスサーバの負荷状態及びサービスサーバを収容するネットワーク装置のトラフィック状態を監視する負荷・トラヒック監視装置と、周期的に負荷・トラヒック監視装置と通信して前記負荷状態及びトラヒック状態の情報を抽出して前記アクセス情報データベースの最大アクセス許容数を算出すると共に、算出した最大アクセス許容数を前記アクセス情報データベースに

登録する動的アクセス許容数算出手段を有するため、サービスサーバの負荷状況やトラヒック状況に応じてサービスサーバが最適に動作可能なアクセス分のユーザにアクセスを許可することが可能となる。

【０１５０】

付記８に記載の発明は、ユーザ端末からのアクセス要求情報を前記アクセスリストから読み出す際に読み出す指針となる制御情報を保持する制御情報データベースと、フィルタリング最適化手段が前記アクセスリストから最大アクセス許容数分のアクセス要求情報を読み出す際に前記アクセスリストがユーザクラス別に登録されている場合、前記制御情報データベースから抽出された制御情報に基づき前記アクセスリストの各ユーザクラスからアクセス要求情報を読み出すユーザクラス別アクセス要求読出手段を有するため、ユーザクラスに応じて読み出すアクセス要求情報数を可変することができる。

【０１５１】

付記９に記載の発明は、パケットフィルタリング設定情報を生成する際にアクセス要求情報に有効タイマを設定する有効タイマ設定手段と、有効タイマの満了時にネットワーク装置に設定したパケットフィルタリング制御を解除するフィルタリング解除手段を有するため、有効タイマを用いて各アクセスの時間管理を行い、アクセス許可を解除することができる。

【０１５２】

付記１０に記載の発明は、ユーザ端末とのセッションを終了したこと判定するセッション終了判定手段と、ユーザ端末とのセッションを終了したことをアクセス制御サーバに通知するセッション終了通知手段を有するため、セッションが終了したアクセスのアクセス許可を解除することができる。

【０１５３】

付記１１に記載の発明は、ユーザクラス抽出手段で抽出したユーザクラスに基づき前記アクセス受付手段を介し受信したアクセス要求が不許可のユーザからか否かを判定し、不許可ユーザであればアクセス制御サーバにその旨を通知するユーザ認証手段を有し、また、付記１２に記載の発明は、受付サーバのユーザ認証手段からの通知に基づき前記サービスサーバにアクセス不許可とするパケットフ

ィルタリング設定情報を生成して前記ネットワーク装置に設定するアクセス不許可フィルタリング設定手段を有するため、ユーザがアクセス権限を持っている場合にのみサービスサーバのアクセスを許可することができる。

【図面の簡単な説明】

【図１】

本発明方法の一実施例の全体構成図である。

【図２】

本発明方法のパケットフィルタリング機能を説明するための図である。

【図３】

本発明方法の予測待合時間通知機能を説明するための図である。

【図４】

本発明方法の予測待合時間通知機能を説明するための図である。

【図５】

本発明方法の動的アクセス許容数算出機能を説明するための図である。

【図６】

本発明方法のユーザクラス別アクセス要求読出機能を説明するための図である。

【図７】

本発明方法の有効タイマ機能を説明するための図である。

【図８】

本発明方法のセッション終了機能を説明するための図である。

【図９】

本発明方法のアクセス不許可機能を説明するための図である。

【図１０】

インターネットサービスプロバイダが受付代行サービスを行う実施例のシステム構成図である。

【図１１】

ユーザプロファイル１１１のデータ構造を示す図である。

【図１２】

アクセス情報ＤＢ２０９のデータ構造を示す図である。

【図１３】

アクセスリスト１０９のデータ構造を示す図である。

【図１４】

制御情報ＤＢ２１１を示す図である。

【図１５】

静的アクセス許容数算出手段２０６が実行する処理のフローチャートである。

【図１６】

アクセス要求情報のメッセージ構造を示す図である。

【図１７】

アクセス登録手段１０３の処理を詳細に説明するためのフローチャートである。

【図１８】

アクセス登録手段１０３の処理を詳細に説明するためのフローチャートである。

【図１９】

フィルタリング要求のメッセージ構造を示す図である。

【図２０】

フィルタリング最適化手段２０４の処理を詳細に説明するためのフローチャートである。

【図２１】

フィルタリング最適化手段２０４の処理を詳細に説明するためのフローチャートである。

【図２２】

フィルタリング・コマンド実行要求のメッセージ構造を示す図である。

【図２３】

トラヒック制御手段２１０の処理を詳細に説明するためのフローチャートである。

【図２４】

有効タイマ設定手段２０３の処理を詳細に説明するためのフローチャートである。

【図２５】

フィルタリング解除手段２０２の処理を詳細に説明するためのフローチャートである。

【図２６】

セッション終了通知手段３０１の処理を詳細に説明するためのフローチャートである。

【図２７】

セッション終了通知のメッセージ構造を示す図である。

【図２８】

セッション完了フィルタリング解除手段２０８の処理を詳細に説明するためのフローチャートである。

【図２９】

アクセス確認手段１０４の処理を詳細に説明するためのフローチャートである。

【図３０】

待合せ確認通知手段１０５の処理を詳細に説明するためのフローチャートである。

【図３１】

予測待合時間算出手段１０６の処理を詳細に説明するためのフローチャートである。

【図３２】

アクセス情報通知手段１０７の処理を詳細に説明するためのフローチャートである。

【図３３】

動的アクセス許容数算出手段２０７の処理を詳細に説明するためのフローチャートである。

【図３４】

ユーザクラス別アクセス登録手段１０８の処理を詳細に説明するためのフローチャートである。

【図３５】

ユーザクラス抽出手段１０２の処理を詳細に説明するための図である。

【図３６】

ユーザクラス別アクセス要求読出手段２０５の処理を詳細に説明するためのフローチャートである。

【図３７】

有効タイマ設定要求のメッセージ構造を示す図である。

【図３８】

ユーザ認証手段１０１の処理を詳細に説明するためのフローチャートである。

【図３９】

アクセス不許可フィルタリング設定手段２０１の処理を詳細に説明するためのフローチャートである。

【符号の説明】

１０　コアネットワーク

２０，３０，４０　ネットワーク装置

５０　ユーザ端末

１００　受付サーバ

３００　サービスサーバ

１０２　ユーザクラス抽出手段

１０３　アクセス登録手段

１０４　アクセス確認手段

１０５　待合せ確認通知手段

１０６　予測待合時間算出手段

１０７　アクセス情報通知手段

１０８　ユーザクラス別アクセス登録手段

１０９　アクセスリスト

１１０　アクセス受付手段

１１１　ユーザプロファイル

２００　アクセス制御サーバ

２０１　アクセス不許可フィルタリング設定手段

２０２　フィルタリング解除手段

２０３　有効タイマ設定手段

２０４　フィルタリング最適化手段

２０５　ユーザクラス別アクセス要求読出手段

２０６　静的アクセス許容数算出手段

２０７　動的アクセス許容数算出手段

２０８　セッション完了フィルタリング解除手段

２０９　アクセス情報ＤＢ

２１０　トラヒック制御手段

２１１　制御情報ＤＢ

２１２　負荷・トラヒック監視装置

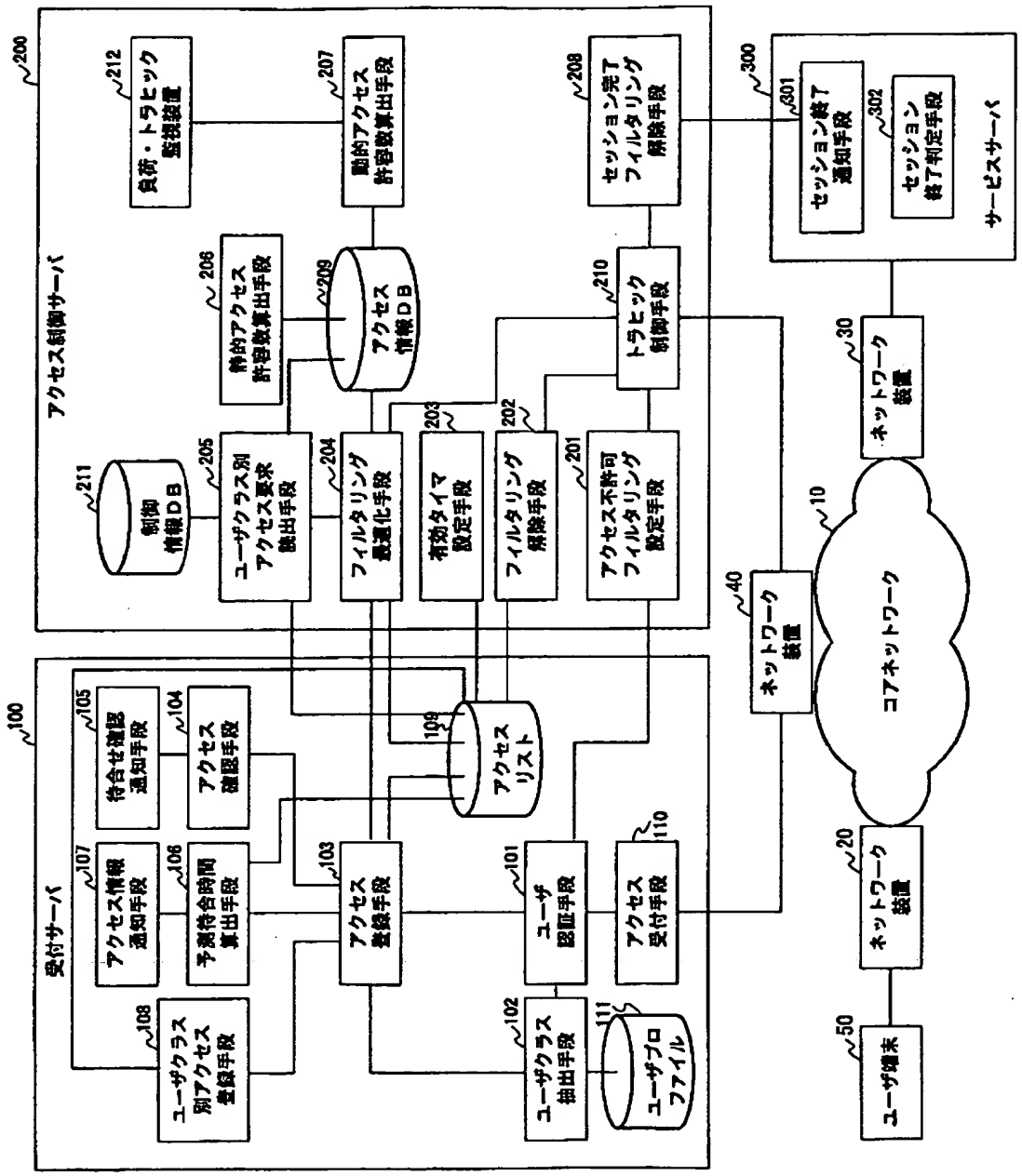
３０１　セッション終了通知手段

３０２　セッション終了判定手段

【書類名】　図面

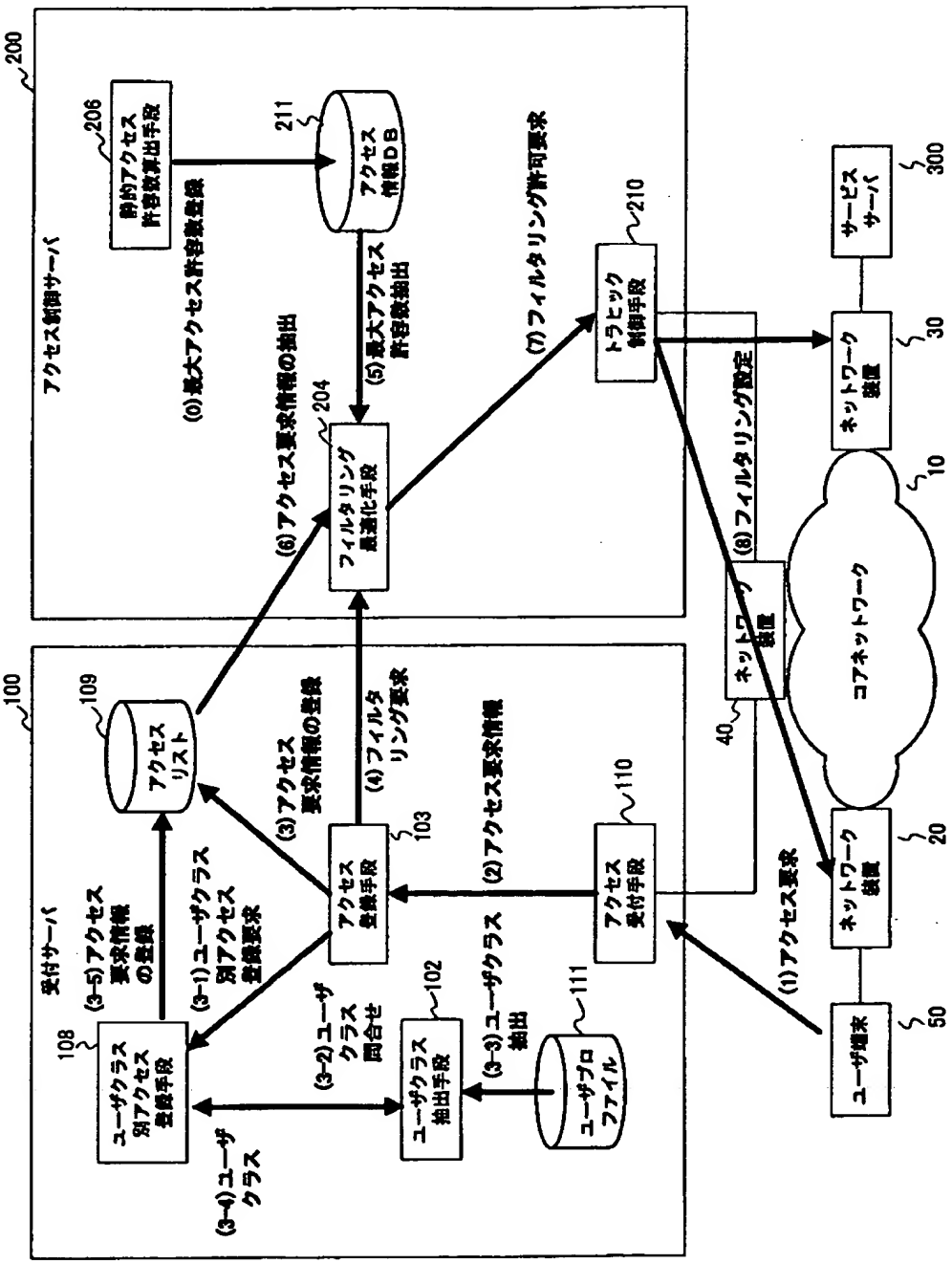
【図１】

本発明方法の一実施例の全体構成図



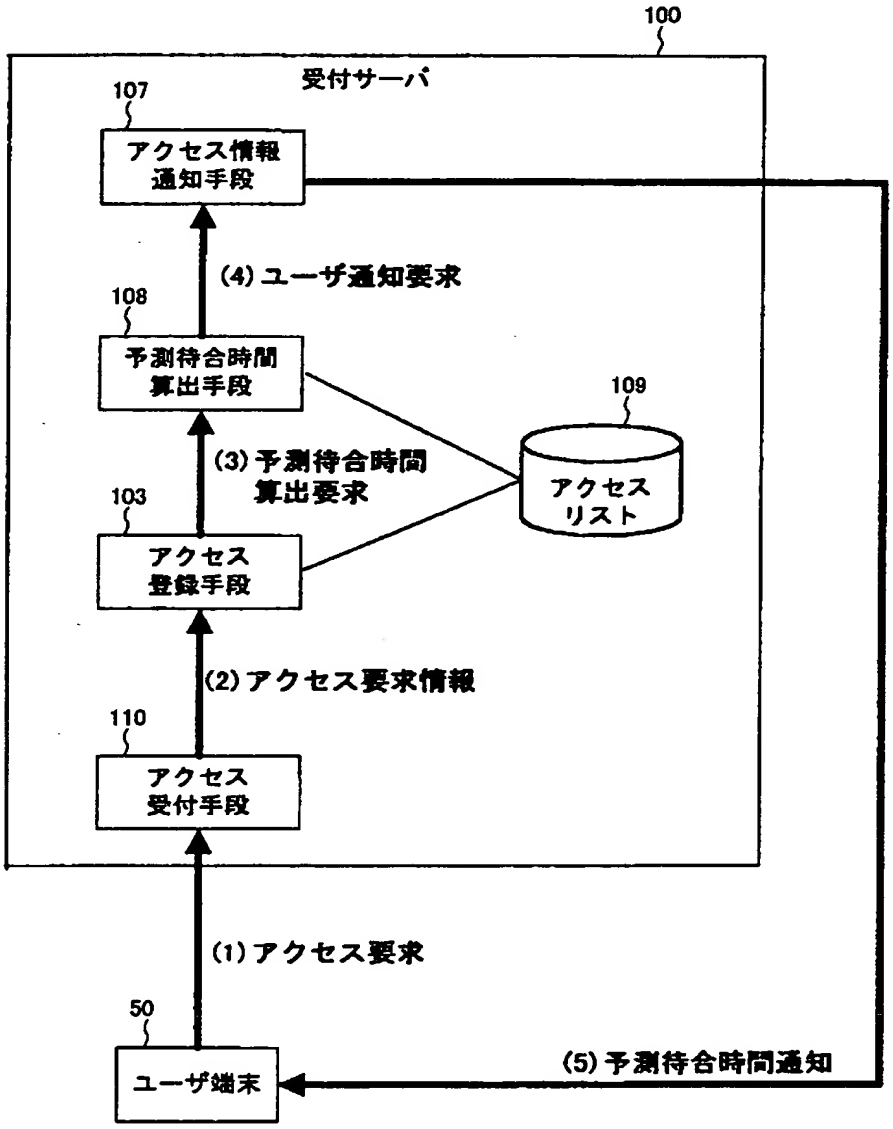
【図２】

本発明方法のパケットフィルタリング機能を説明するための図



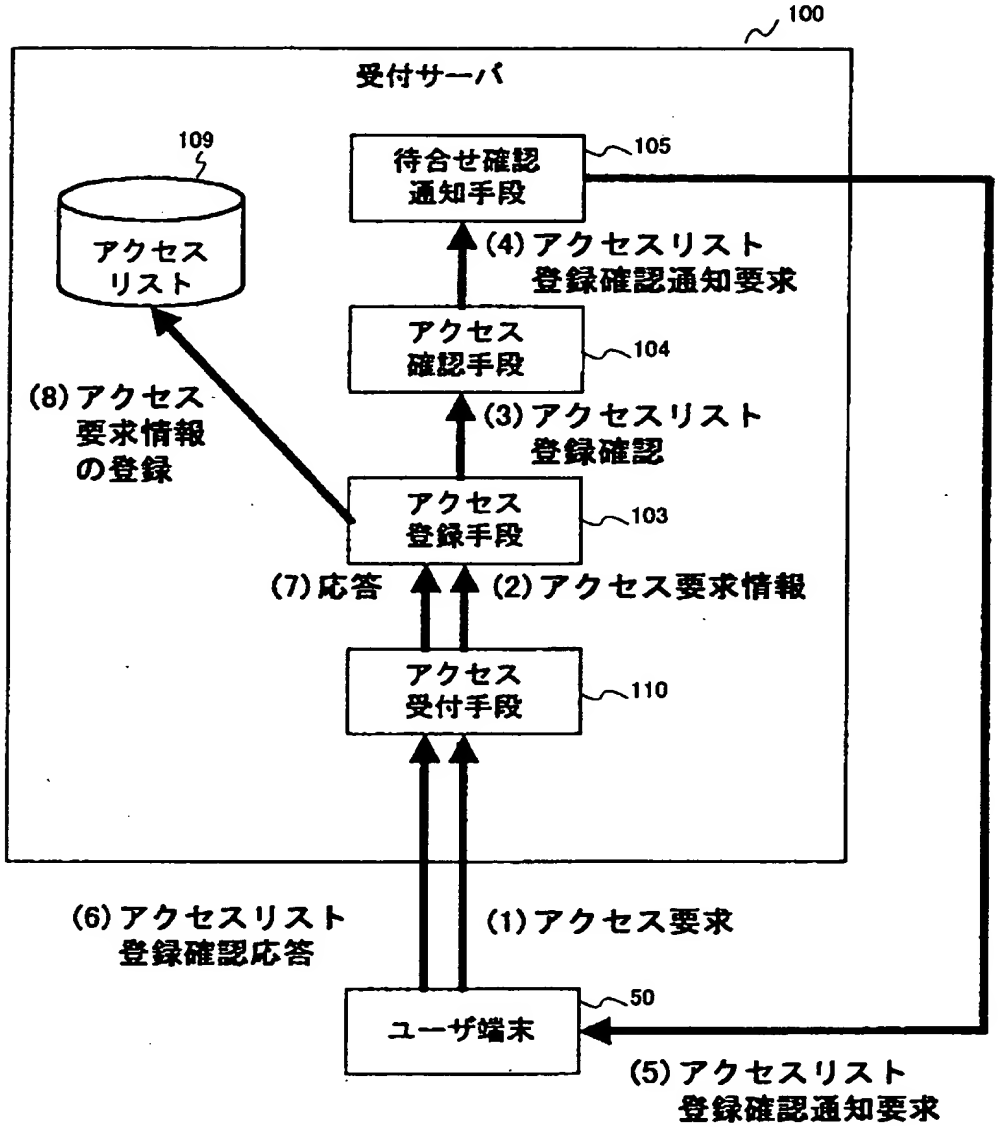
【図３】

本発明方法の予測待合時間通知機能を説明するための図



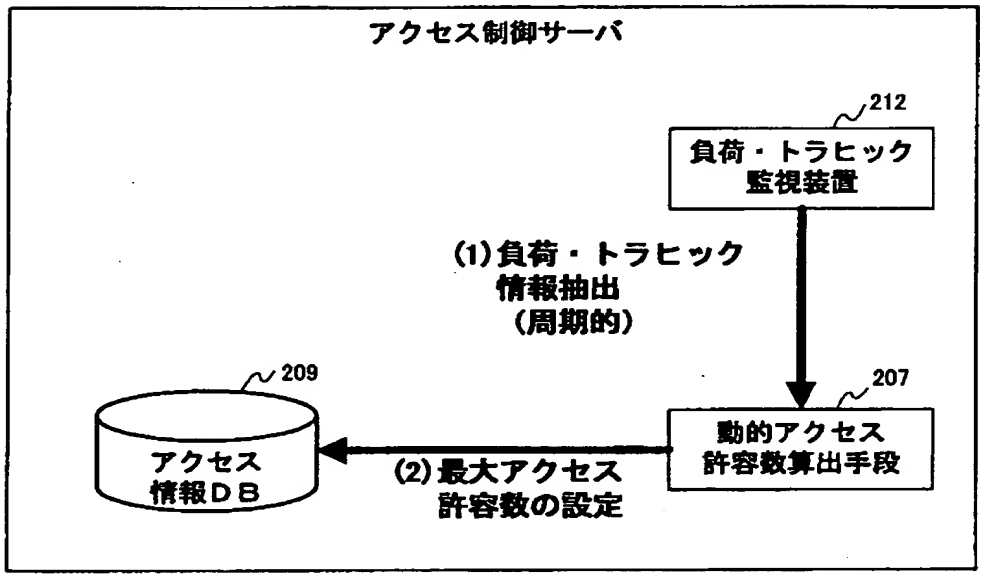
【図４】

本発明方法の予測待合時間通知機能を説明するための図



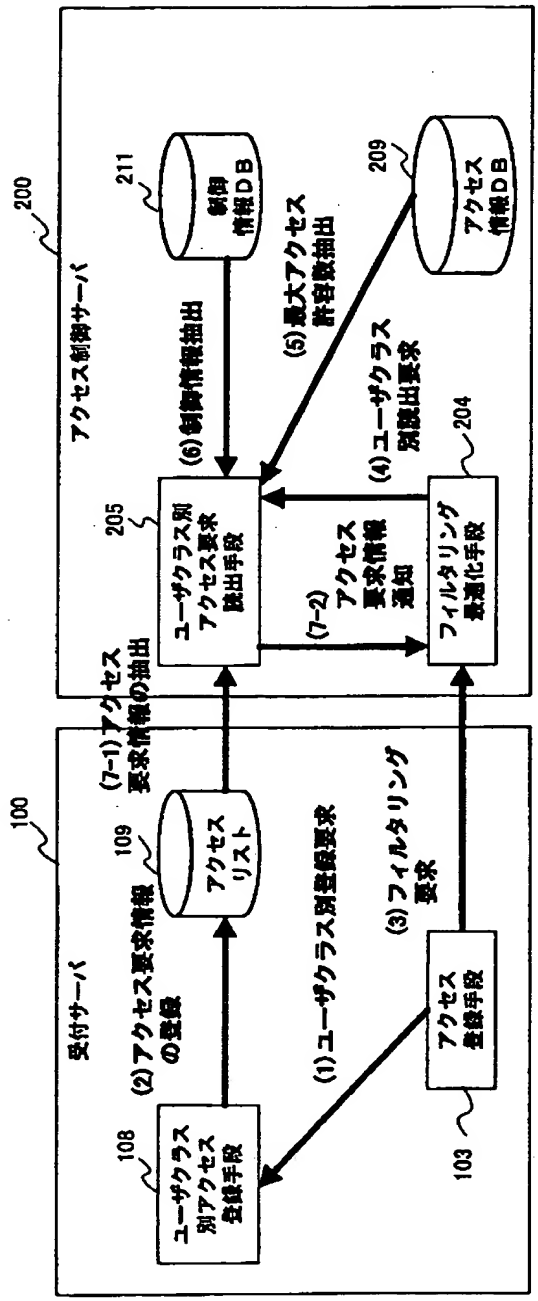
【図５】

本発明方法の動的アクセス許容数算出機能を説明するための図



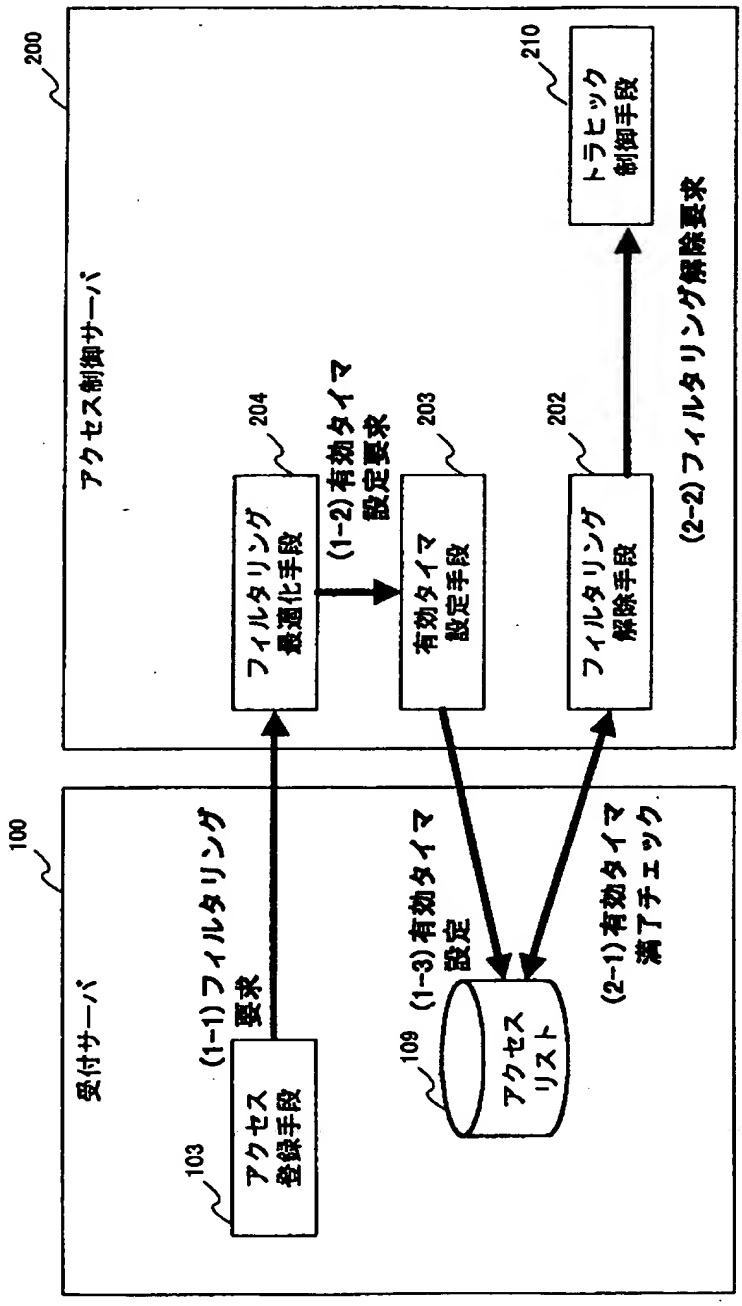
【図６】

本発明方法のユーザクラス別アクセス要求読出機能を説明するための図



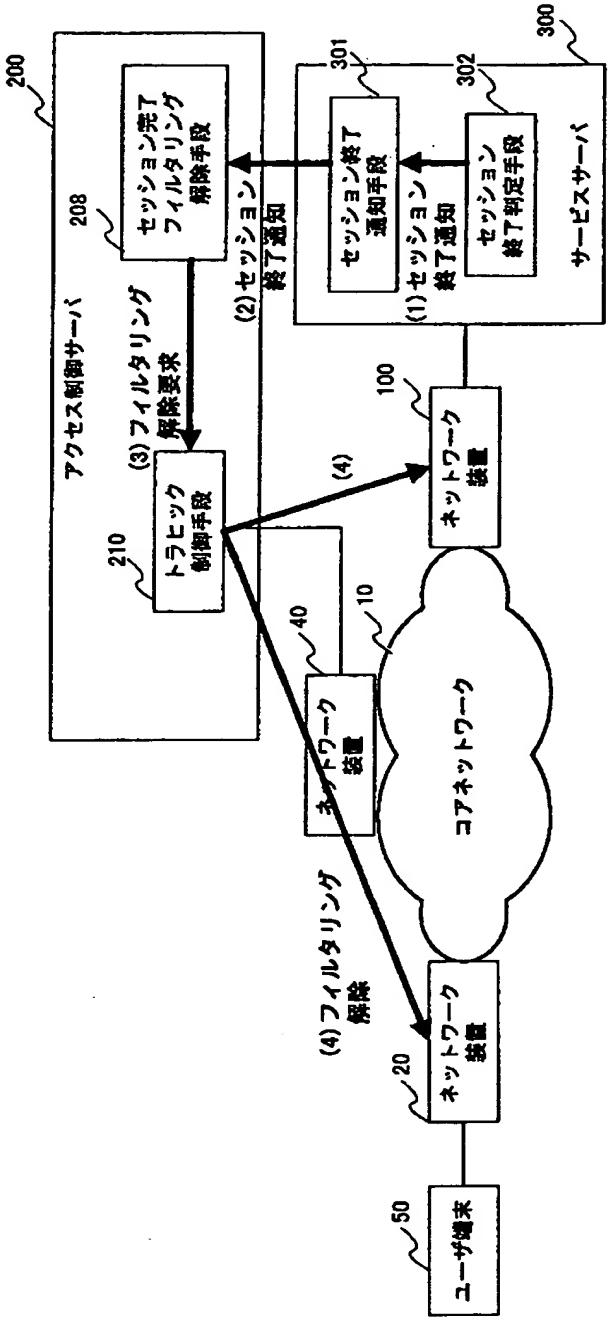
【図７】

本発明方法の有効タイマ機能を説明するための図



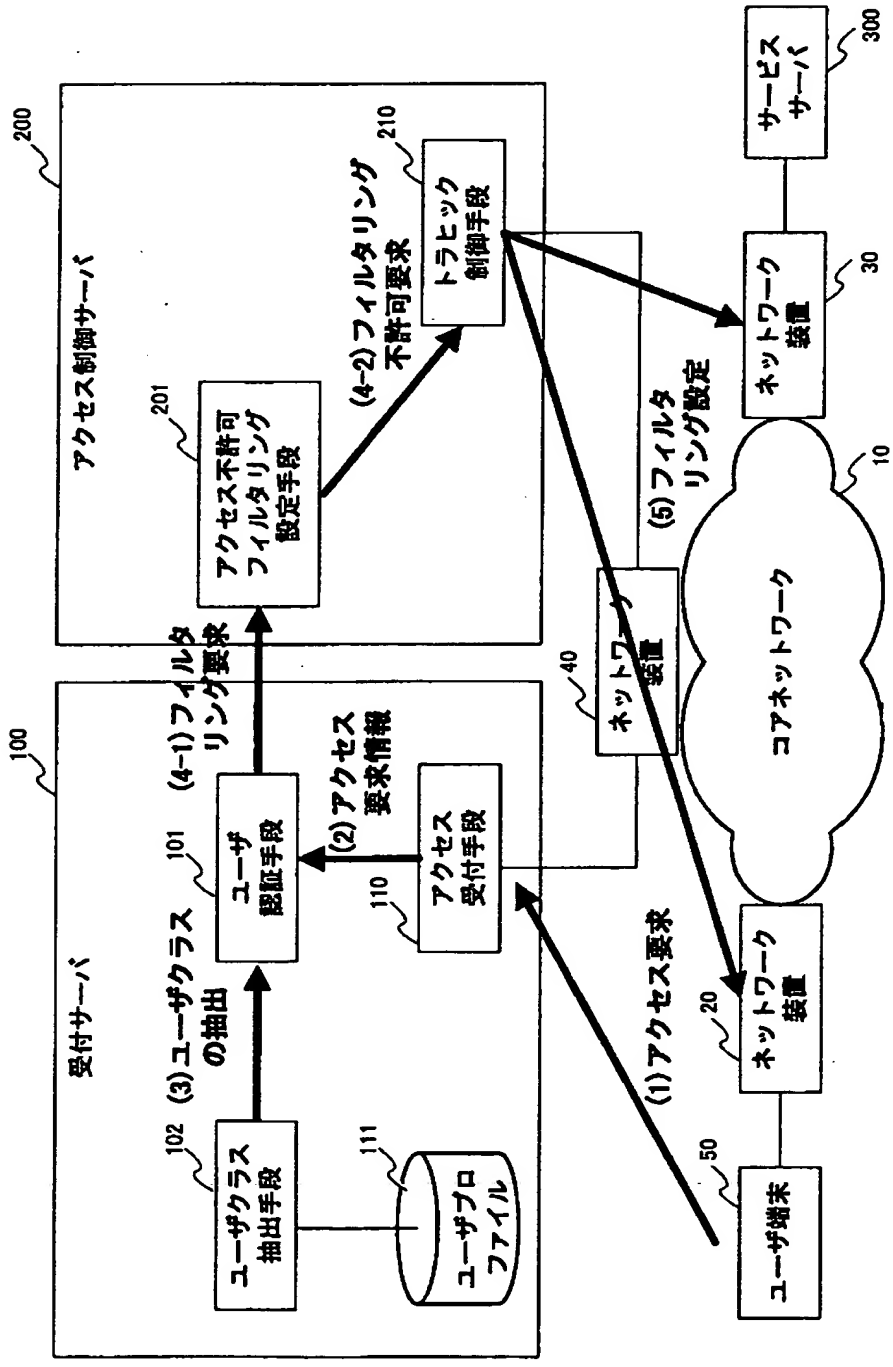
【図８】

本発明方法のセッション終了機能を説明するための図



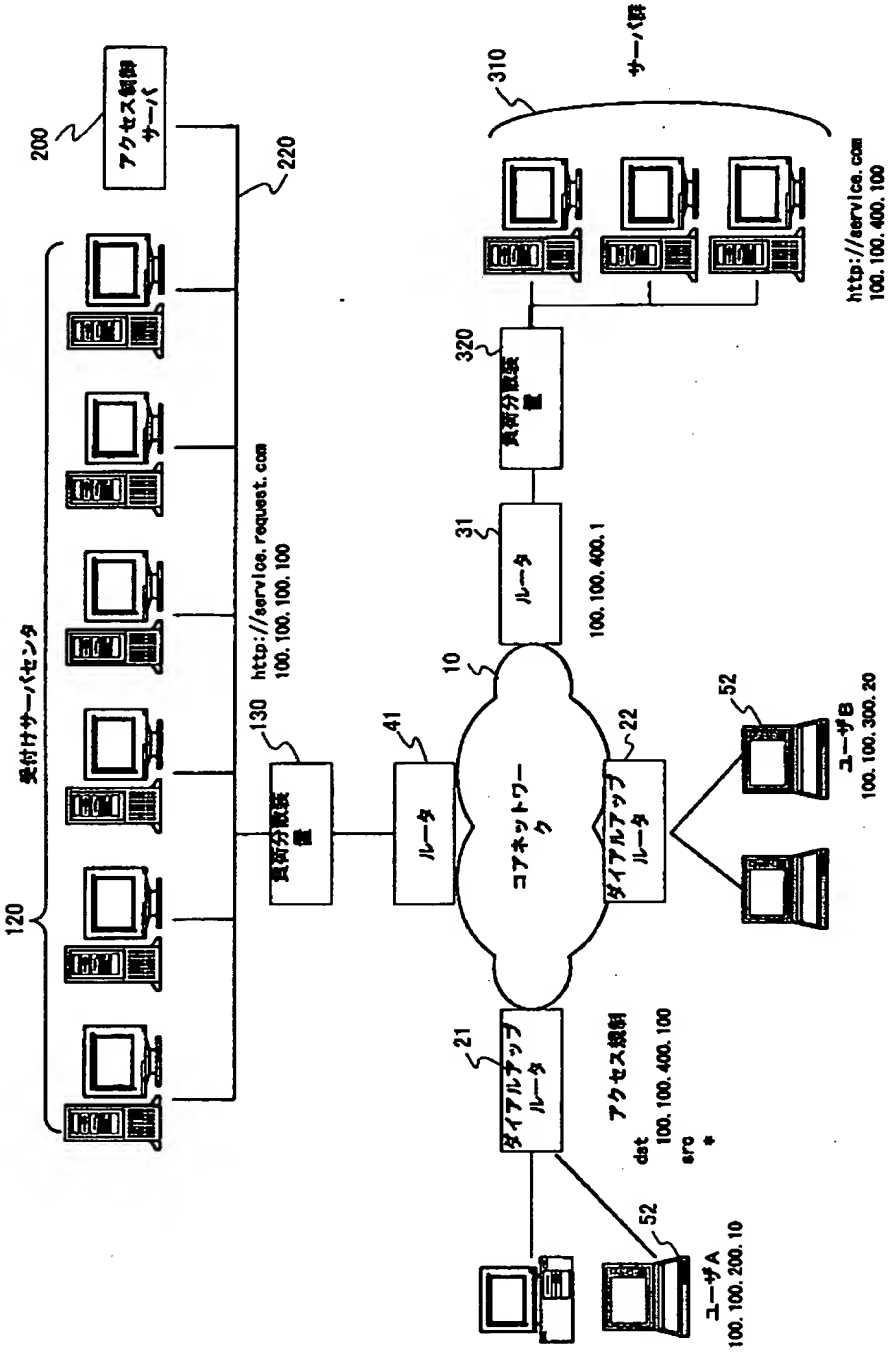
【図９】

本発明方法のアクセス不許可機能を説明するための図



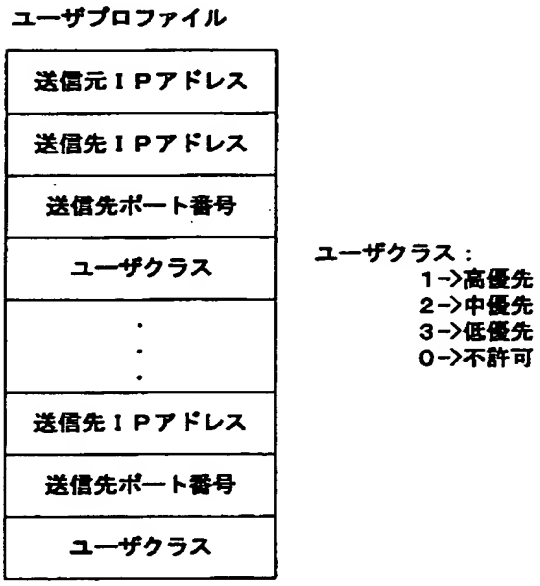
【図１０】

インターネットサービスプロバイダが
受付代行サービスを行う実施例のシステム構成図



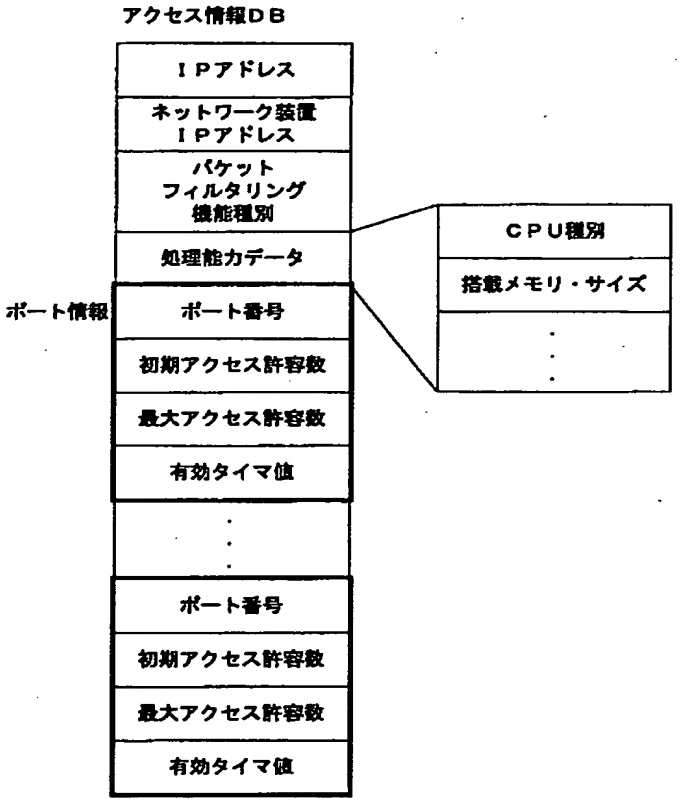
【図１１】

ユーザプロファイル111のデータ構造を示す図



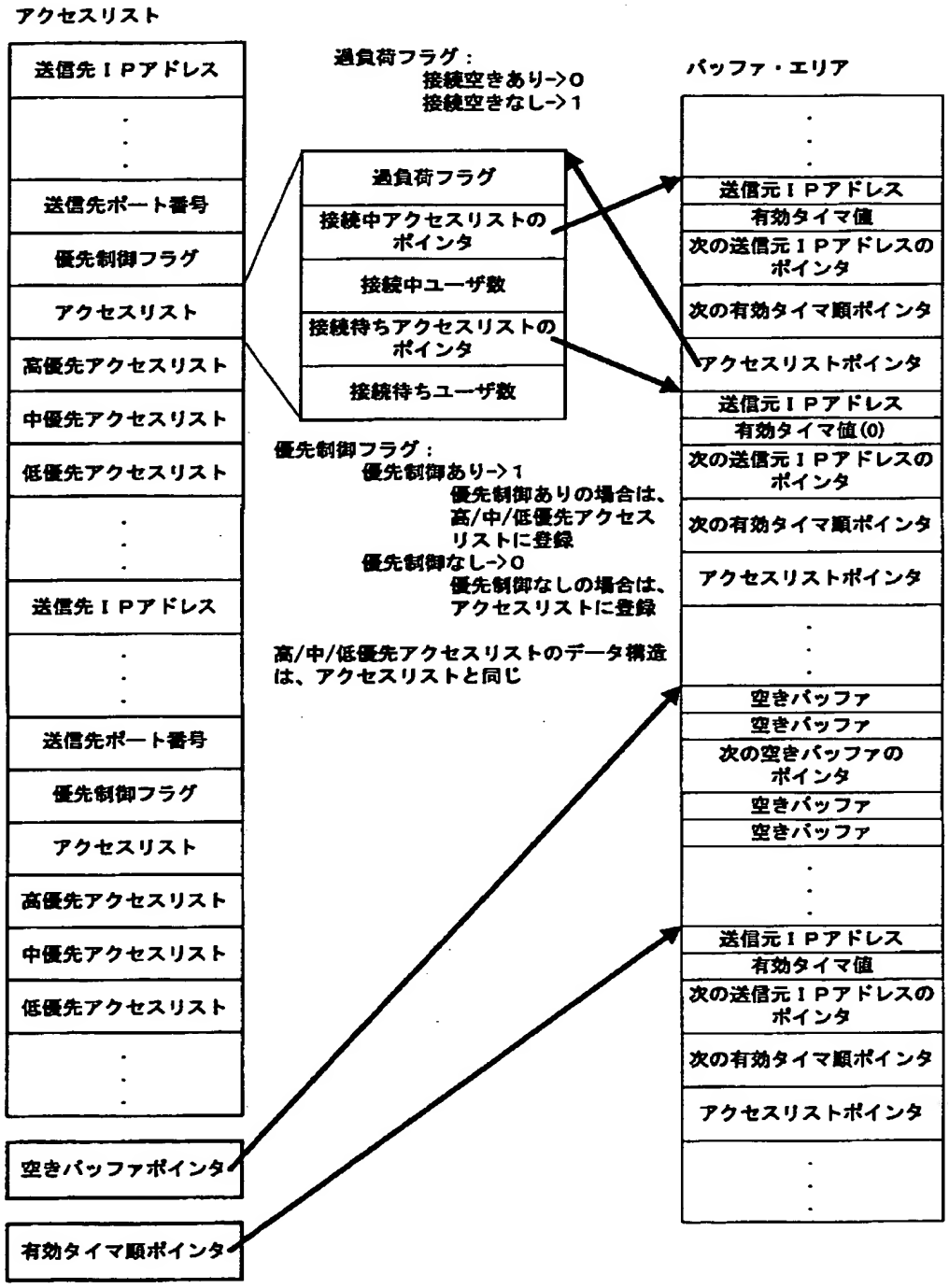
【図１２】

アクセス情報DB209のデータ構造を示す図



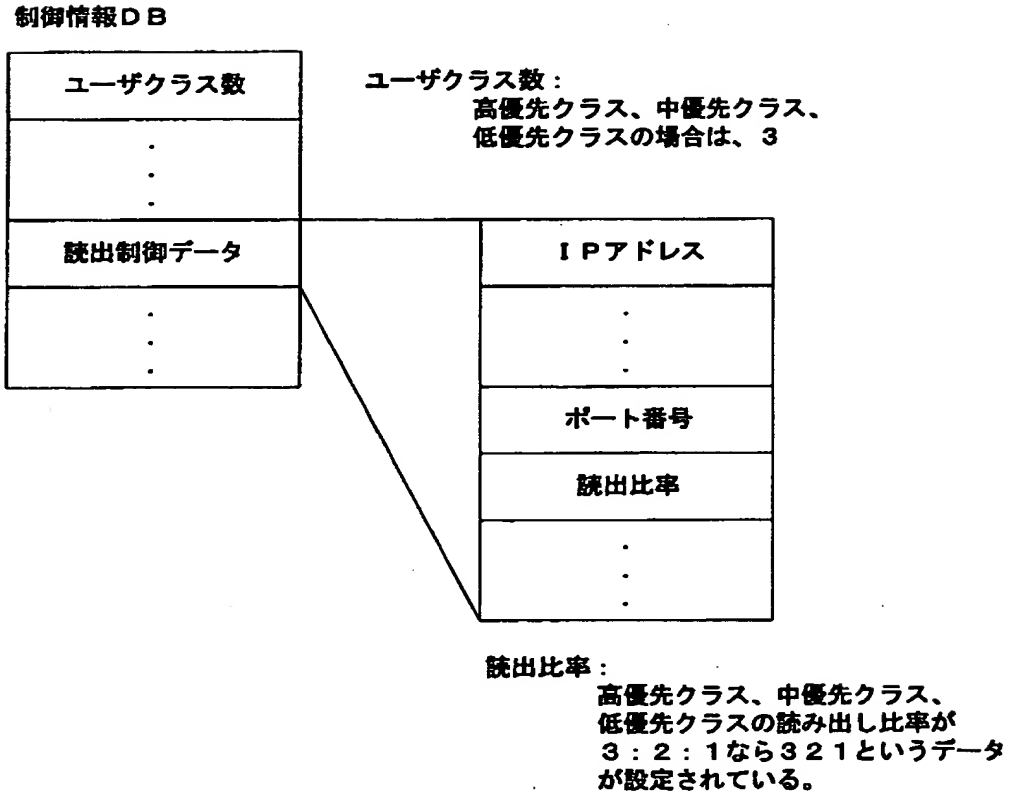
【図１３】

アクセスリスト109のデータ構造を示す図



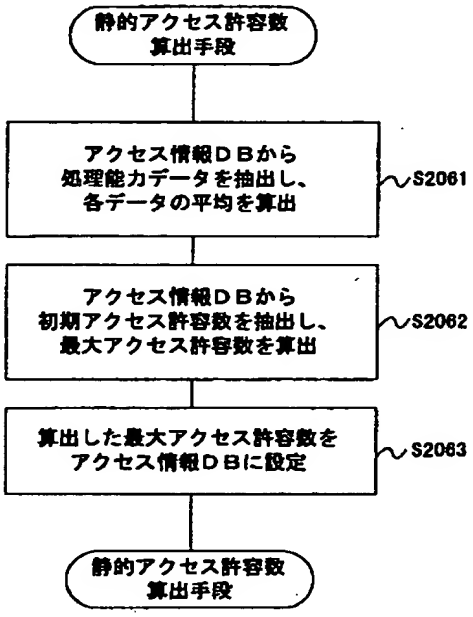
【図１４】

制御情報DB211を示す図



【図１５】

静的アクセス許容数算出手段206が実行する処理のフローチャート図



【図１６】

アクセス要求情報のメッセージ構造を示す図

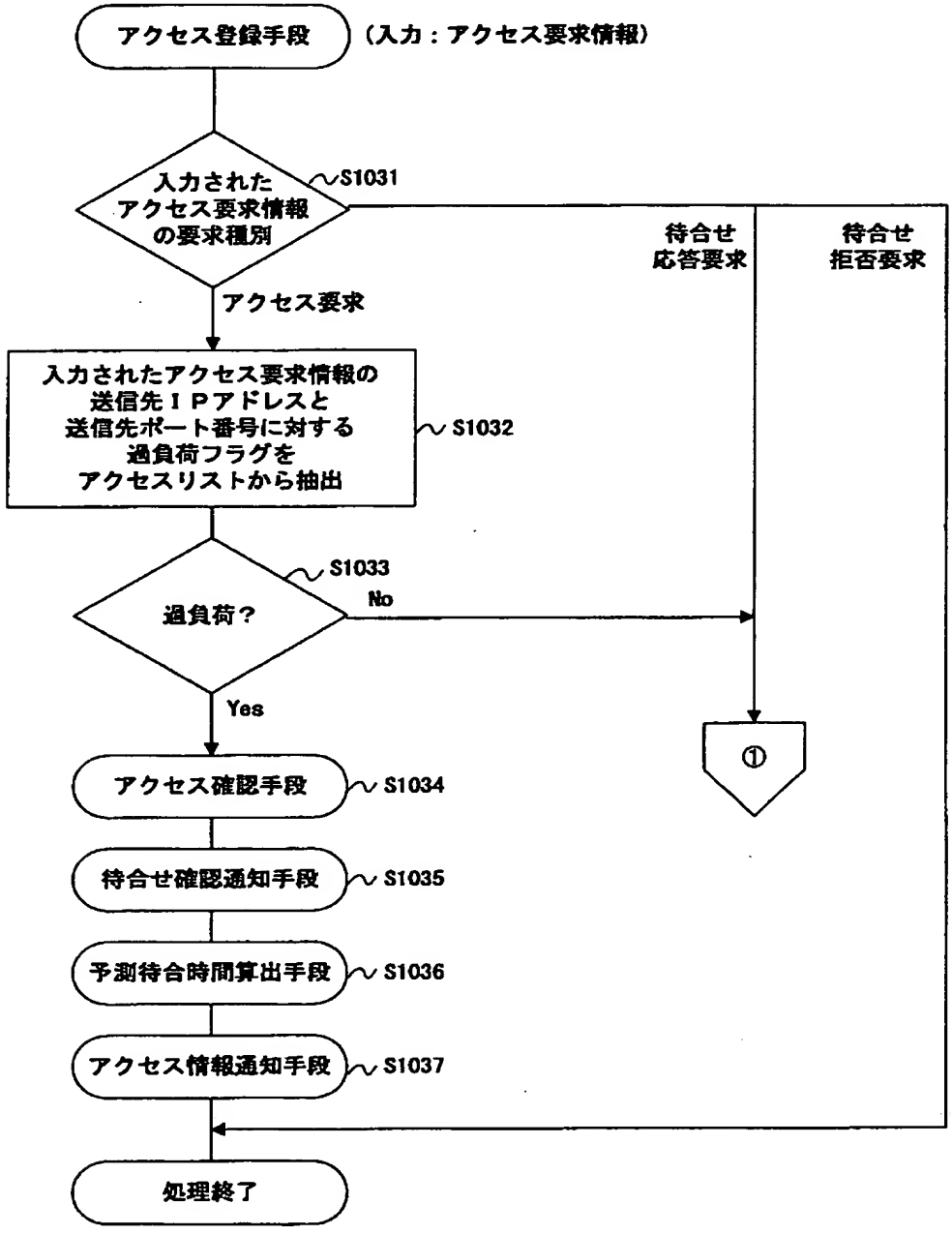
アクセス要求情報

要求種別
送信元ＩＰアドレス
送信先ＩＰアドレス
送信先ポート番号

要求種別：
アクセス要求->０
待合せ応答要求->１
待合せ拒否要求->２

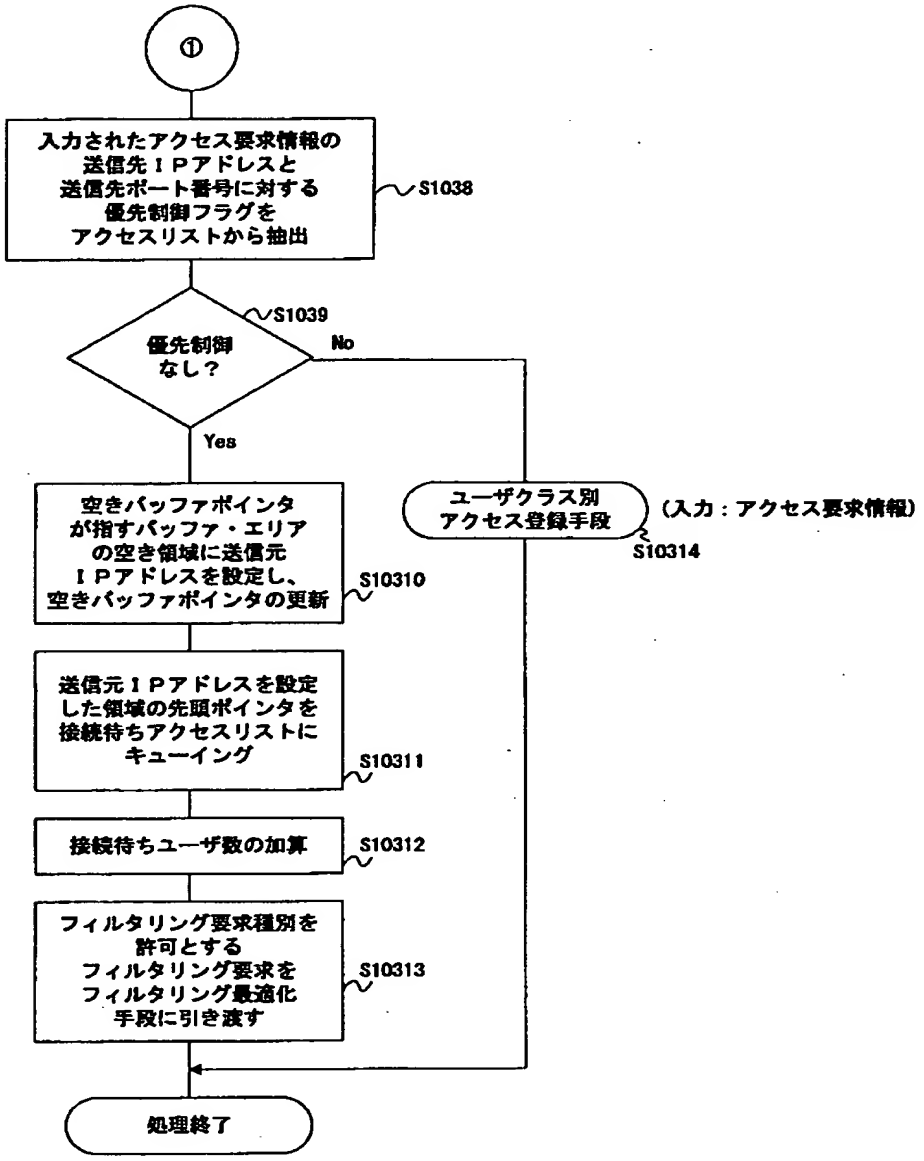
【図１７】

アクセス登録手段103の処理を詳細に説明するためのフローチャート



【図１８】

アクセス登録手段103の処理を詳細に説明するためのフローチャート



【図１９】

フィルタリング要求のメッセージ構造を示す図

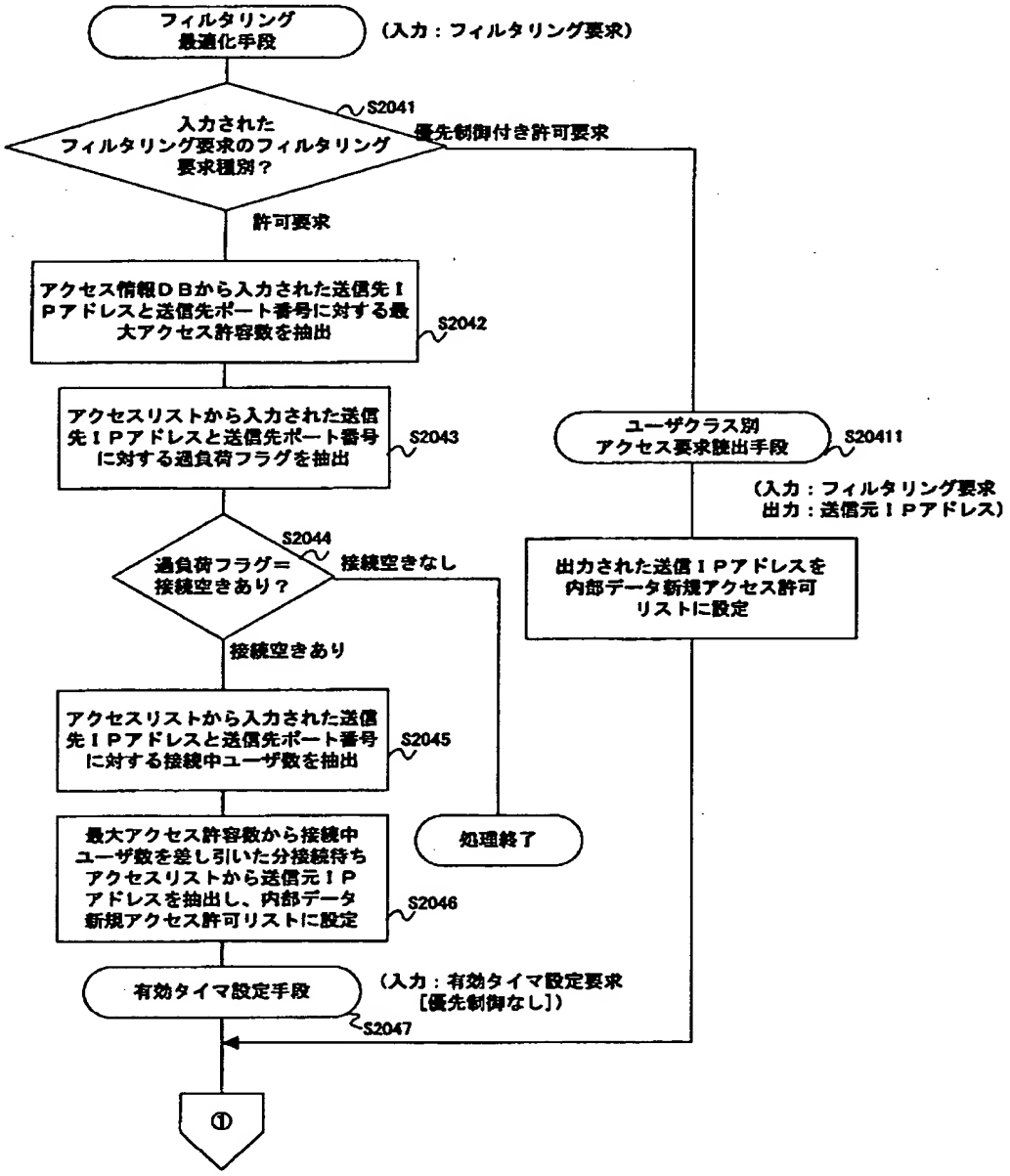
フィルタリング要求

フィルタリング要求種別
送信元ＩＰアドレス
送信先ＩＰアドレス
送信先ポート番号

フィルタリング要求種別：
０：許可要求
１：不許可要求
２：優先制御付き許可要求
３：（許可）解除要求

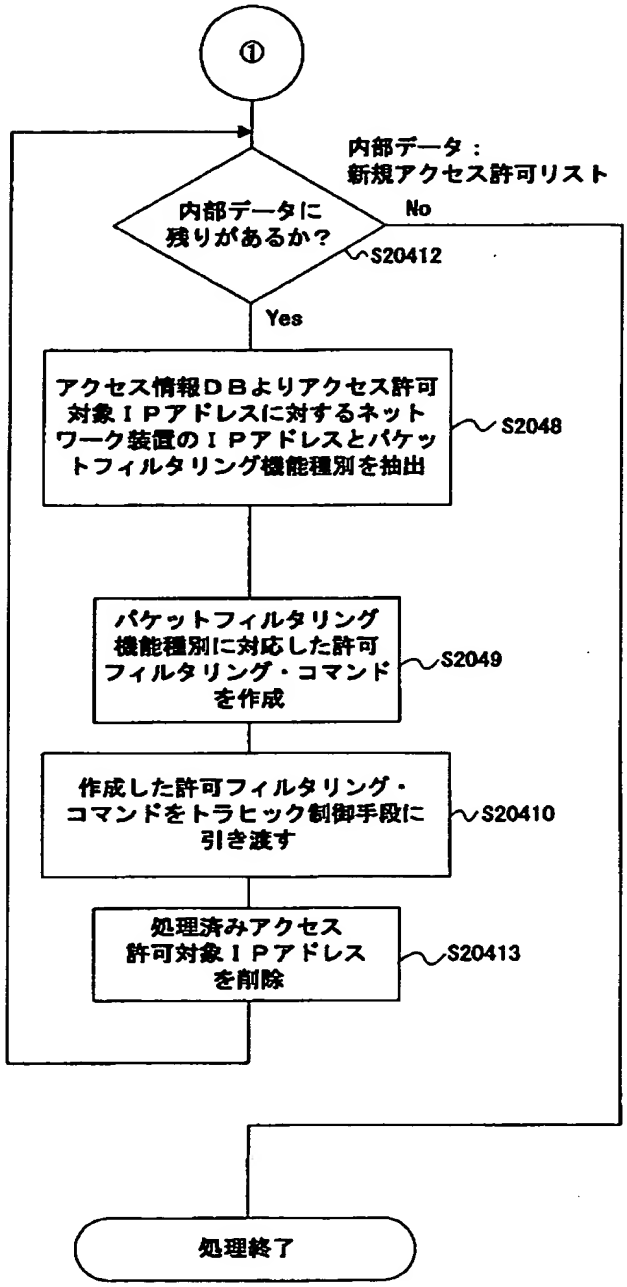
【図２０】

フィルタリング最適化手段204の処理を詳細に説明するためのフローチャート



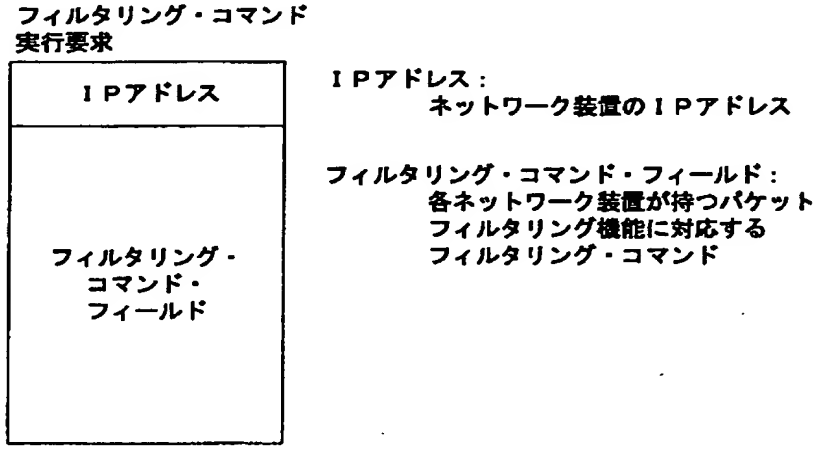
【図２１】

フィルタリング最適化手段204の処理を詳細に説明するためのフローチャート



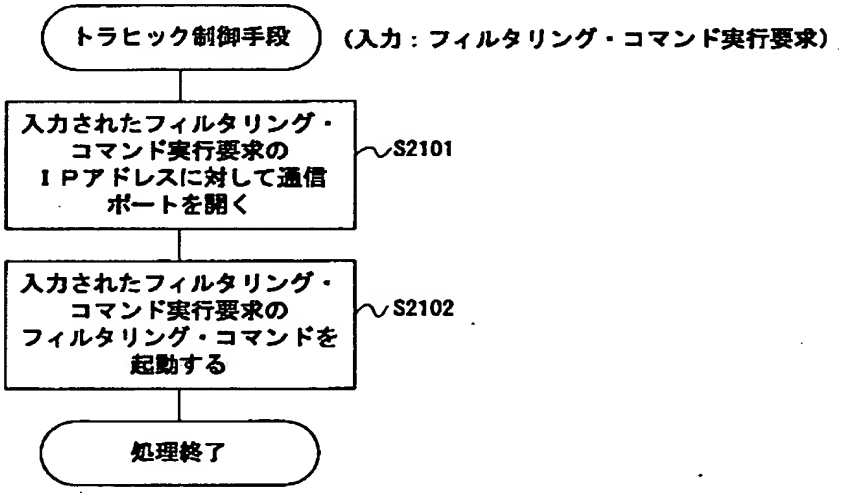
【図２２】

フィルタリング･コマンド実行要求のメッセージ構造を示す図



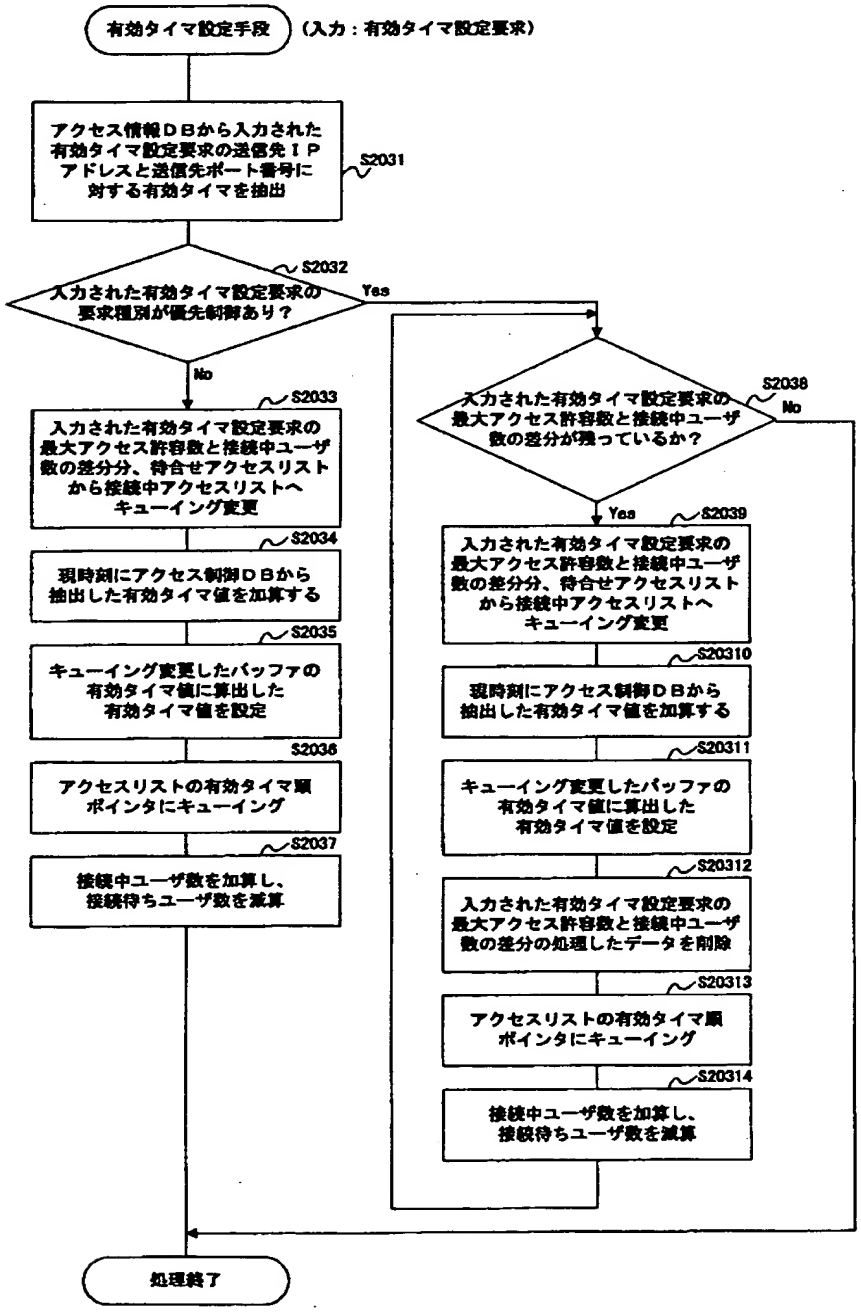
【図２３】

トラヒック制御手段210の処理を詳細に説明するためのフローチャート



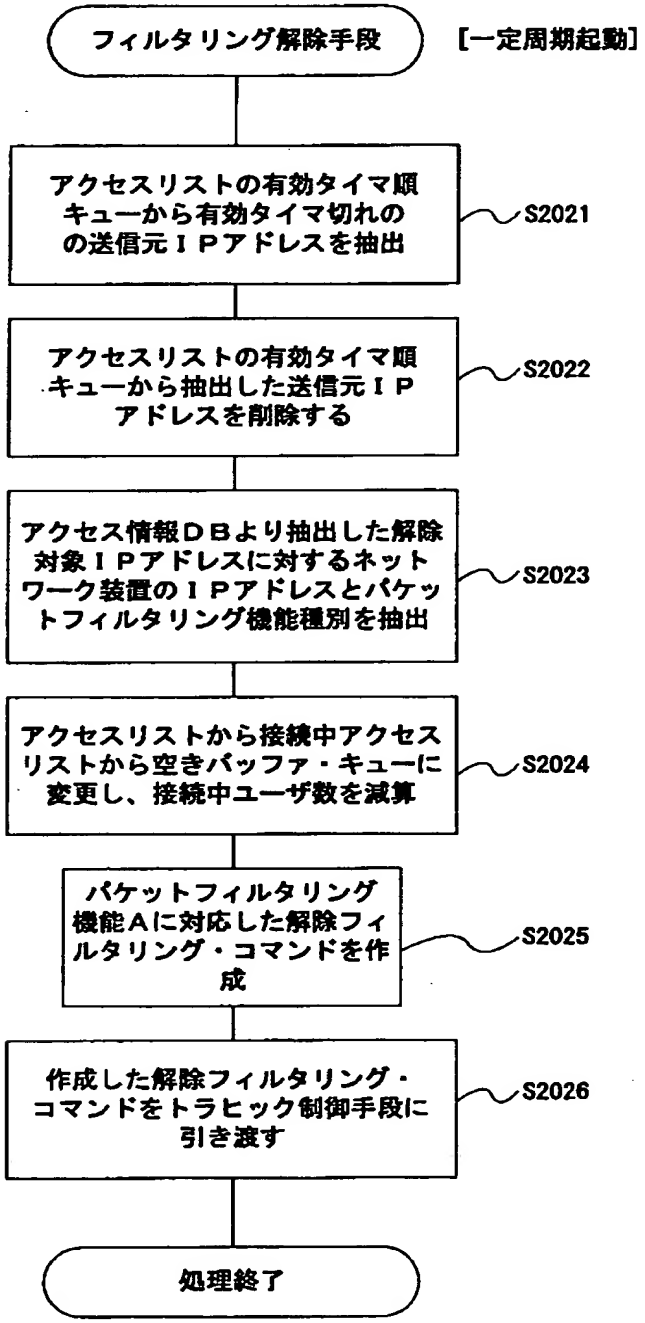
【図２４】

有効タイマ設定手段203の処理を詳細に説明するためのフローチャート



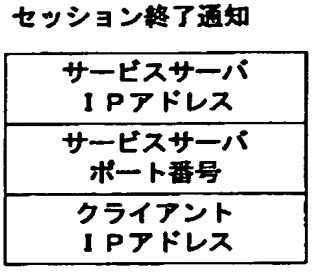
【図２５】

フィルタリング解除手段202の処理を詳細に説明するためのフローチャート



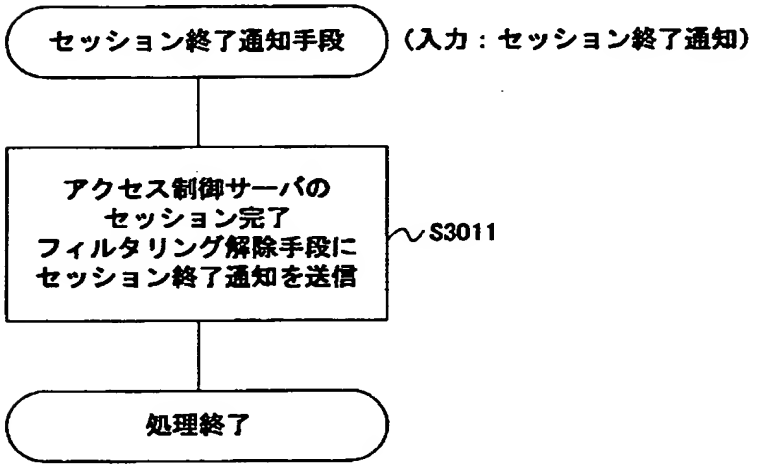
【図２６】

セッション終了通知手段301の処理を詳細に説明するためのフローチャート



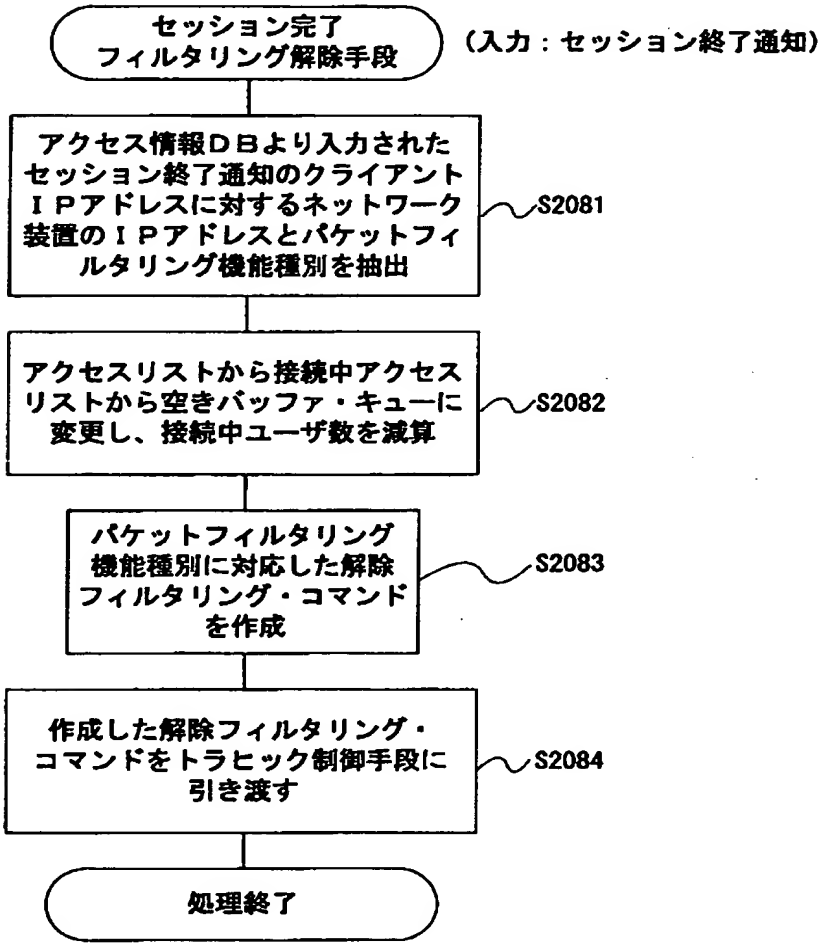
【図２７】

セッション終了通知のメッセージ構造を示す図



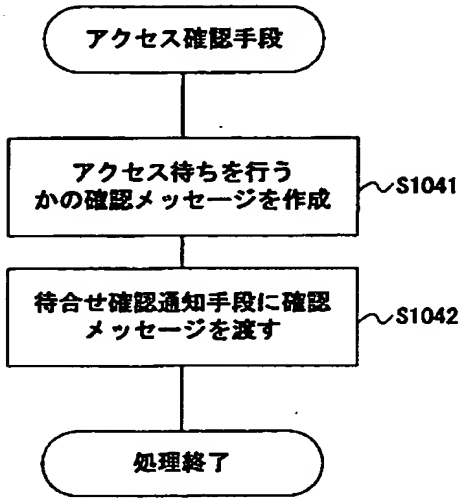
【図２８】

セッション完了フィルタリング解除手段208の処理を
詳細に説明するためのフローチャート



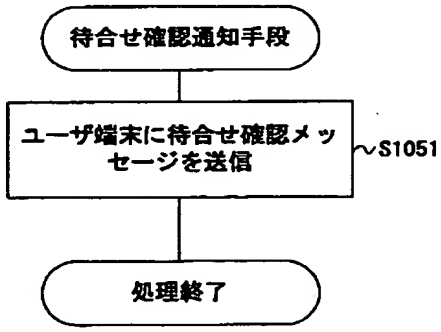
【図２９】

アクセス確認手段104の処理を詳細に説明するためのフローチャート



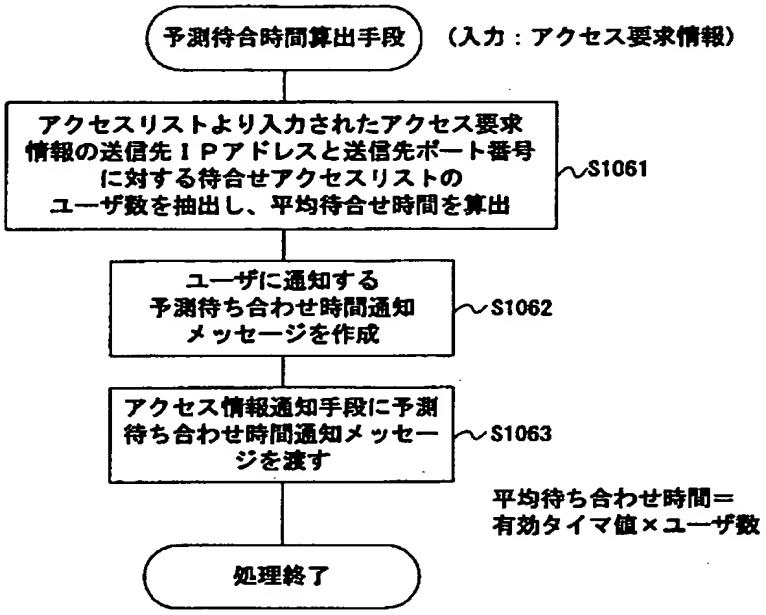
【図３０】

待合せ確認通知手段105の処理を詳細に説明するためのフローチャート



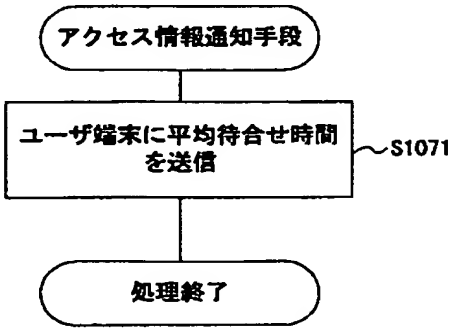
【図３１】

予測待合時間算出手段106の処理を詳細に説明するためのフローチャート



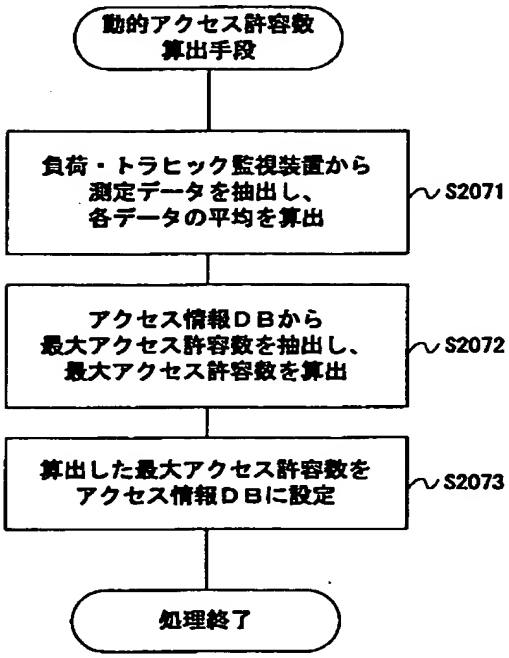
【図３２】

アクセス情報通知手段107の処理を詳細に説明するためのフローチャート



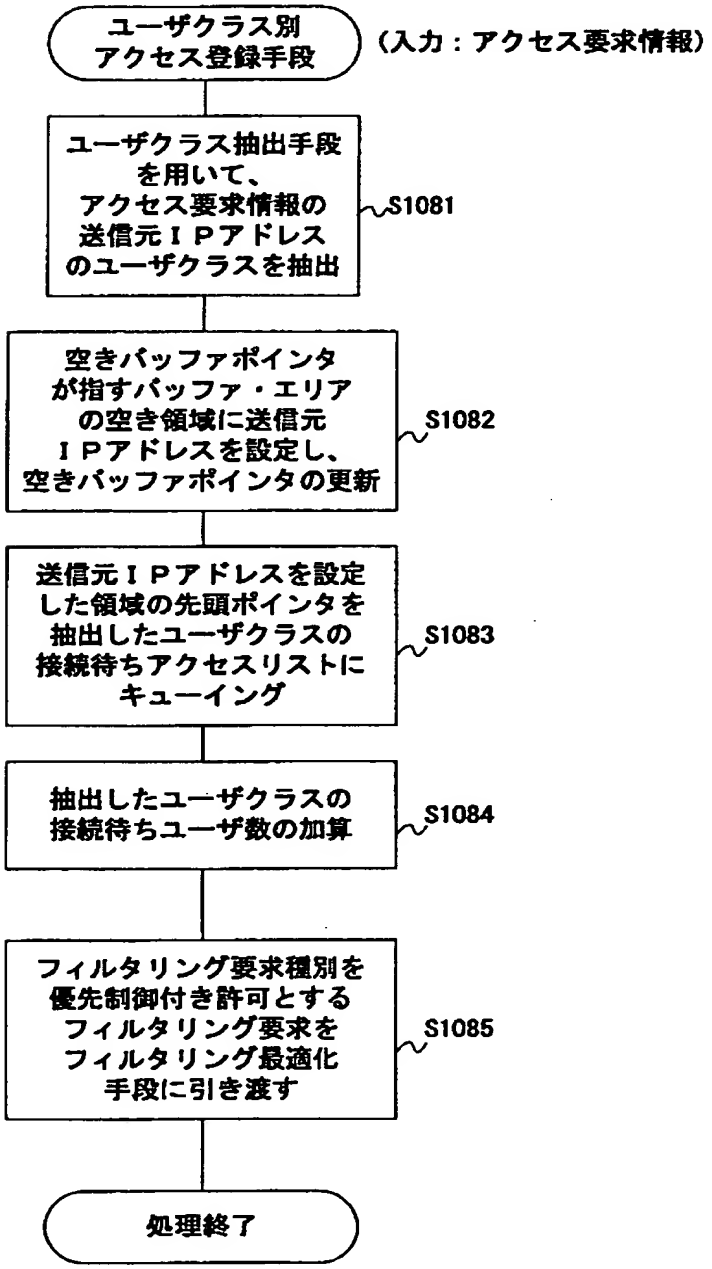
【図３３】

動的アクセス許容数算出手段207の処理を詳細に説明するためのフローチャート



【図３４】

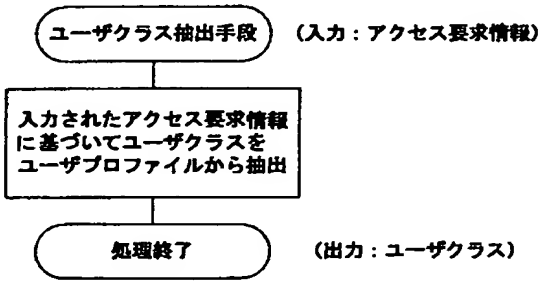
ユーザクラス別アクセス登録手段108の処理を詳細に説明するためのフローチャート



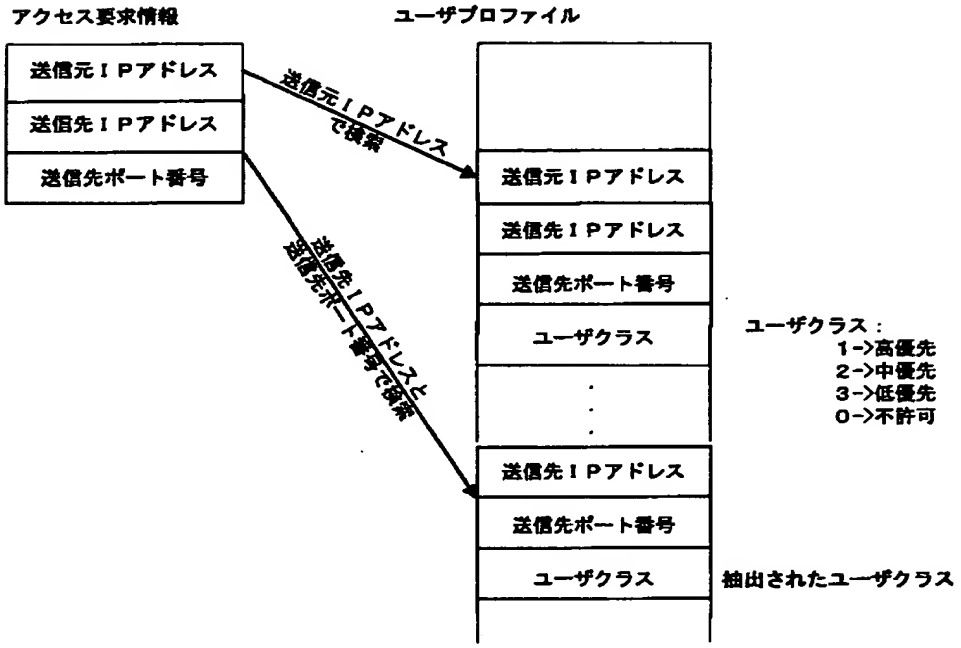
【図３５】

ユーザクラス抽出手段102の処理を詳細に説明する図

(A)

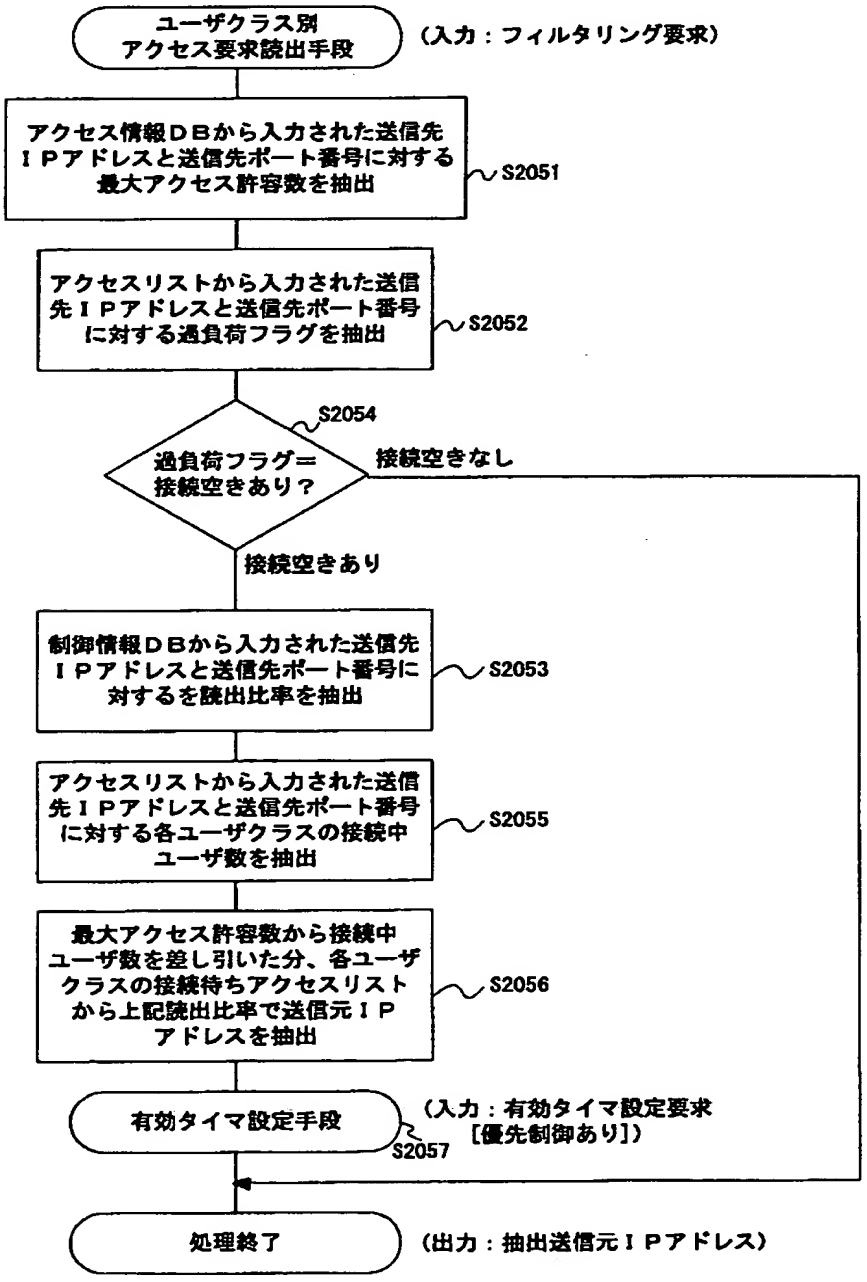


(B)



【図３６】

ユーザクラス別アクセス要求読出手段205の処理を詳細に説明するためのフローチャート



【図３７】

有効タイマ設定要求のメッセージ構造を示す図

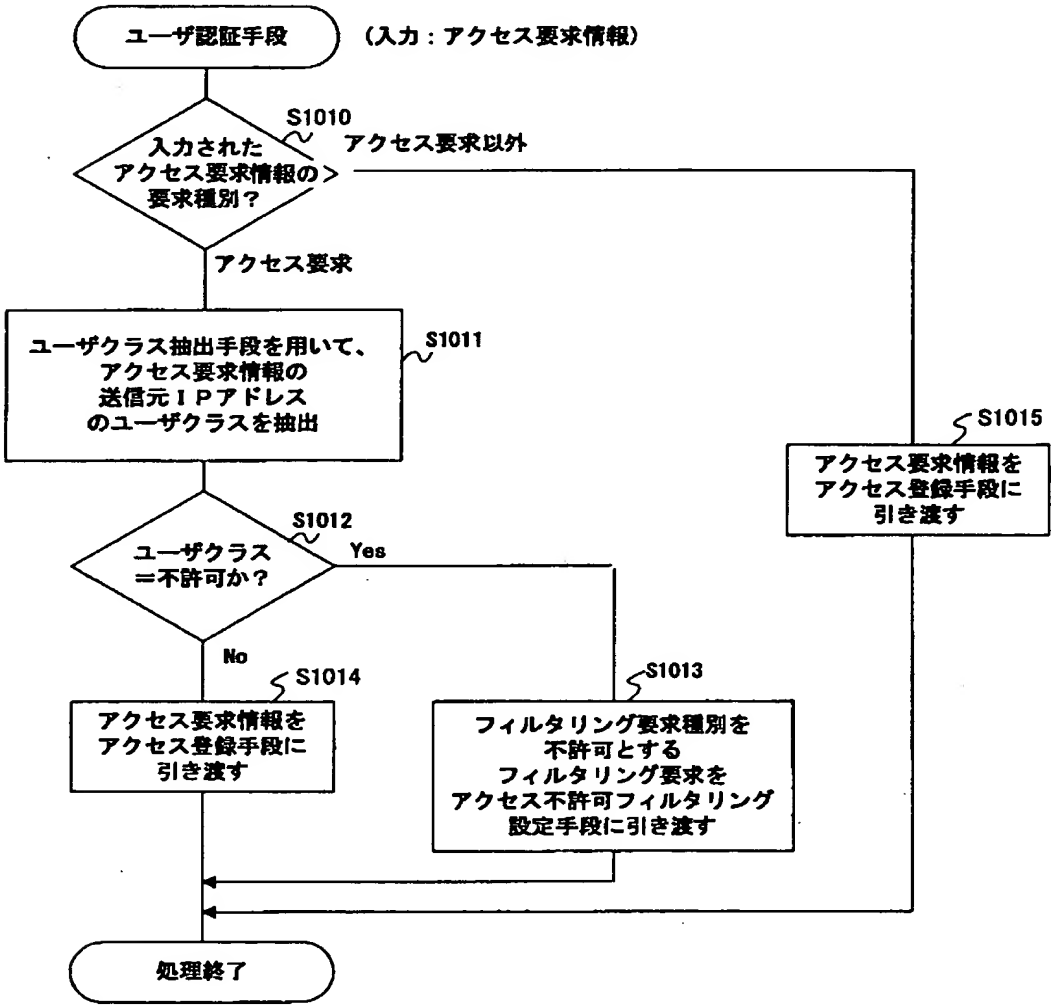
有効タイマ設定要求

要求種別
最大アクセス許容数と接続中ユーザ数との差分
・ ・ ・
最大アクセス許容数と接続中ユーザ数との差分
送信先ＩＰアドレス
送信先ポート番号

要求種別：
優先制御あり->０
優先制御なし->１
最大アクセス許容数と接続中ユーザ数との差分：
優先制御なしの場合は、データは一つ設定
優先制御ありの場合は、ユーザクラス分設定

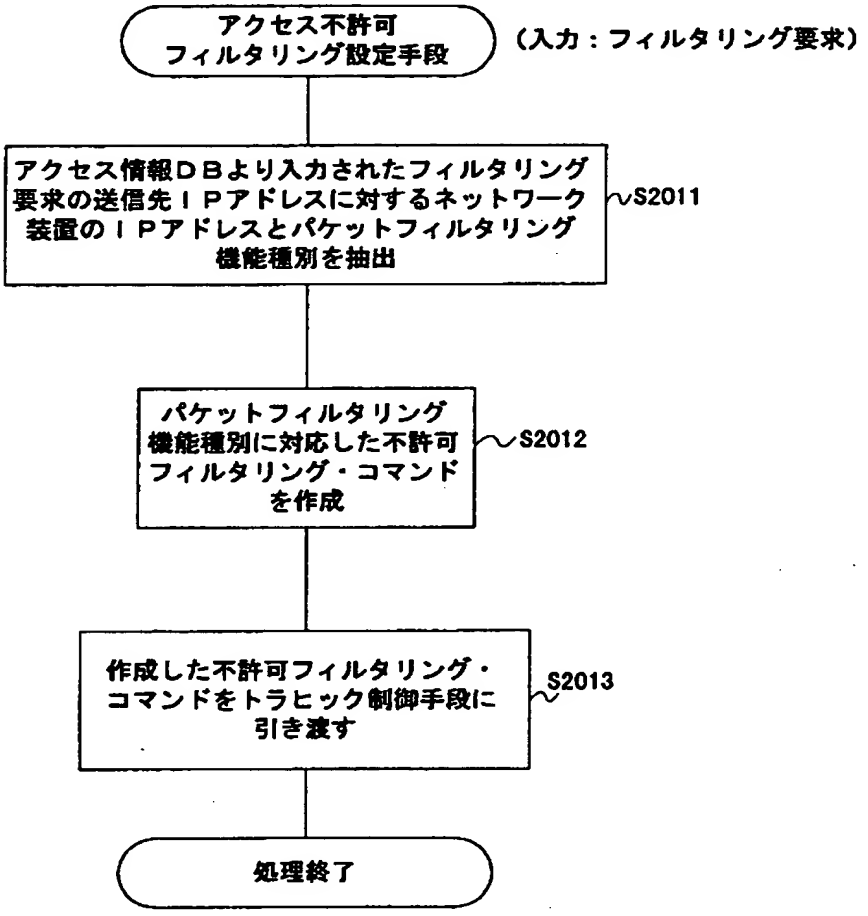
【図３８】

ユーザ認証手段101の処理を詳細に説明するためのフローチャート



【図３９】

アクセス不許可フィルタリング設定手段201の処理を
詳細に説明するためのフローチャート



【書類名】　　要約書

【要約】

【課題】　本発明は、動的オブジェクトを再利用でき、トラヒックの軽減を図ることができ、ユーザに与える負担を軽減でき、アクセス要求したユーザは自分のアクセス順番になれば速い応答速度で快適にサービスを受けることが可能となるネットワークアクセス制御方法及びそれを用いたネットワークシステム及びそれを構成する装置を提供することを目的とする。

【解決手段】　受付サーバ１００は、ユーザ端末５０からのアクセス要求情報を受信して保持し、アクセス制御サーバ２００は、サービスサーバ３００の処理能力及びサービスサーバへのトラヒック量に基づき最適に処理可能なアクセス要求分だけアクセス登録手段１０３に保持されたアクセス要求情報を抽出して前記サービスサーバ３００へのアクセスを許容するトラヒック制御を行うため、ユーザがサービスサーバにアクセスする場合に、サービスサーバ３００の処理能力及びサービスサーバへのトラヒック量に見合う分だけのユーザからのアクセスが許容され、動的オブジェクトを再利用できると共にトラヒックの軽減を図ることができる。

【選択図】　　図１

出　願　人　履　歴　情　報

識別番号　　〔０００００５２２３〕

１．変更年月日　　１９９６年　３月２６日
［変更理由］　住所変更
住　所　神奈川県川崎市中原区上小田中４丁目１番１号
氏　名　富士通株式会社